FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Sistema de Identificação de Objetos e Pessoas para Bancada Laboratorial

Miguel Fernandes

Mestrado Integrado em Engenharia Eletrotécnica e de Computadores

Orientador: Professor Paulo Portugal

Co-orientador: Professor Joaquim Gabriel

29 de Outubro de 2015

U.PORTO
FEUP FACULDADE DE ENGENHARIA UNIVERSIDADE DO PORTO

MIEEC - MESTRADO INTEGRADO EM ENGENHARIA ELETROTÉCNICA E DE COMPUTADORES | **2014/2015**

A Dissertação intitulada

"Sistema de Identificação de Objectos e Pessoas para Bancada Laboratorial"

foi aprovada em provas realizadas em 21-10-2015

o júri

Presidente Professor Doutor Armando Luís Sousa Araújo
Professor Auxiliar do Departamento de Engenharia Eletrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto

Professor Doutor José Alberto Gouveia Fonseca
Professor Associado do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro

Professor Doutor Paulo José Lopes Machado Portugal
Professor Associado do Departamento de Engenharia Eletrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto

O autor declara que a presente dissertação (ou relatório de projeto) é da sua exclusiva autoria e foi escrita sem qualquer apoio externo não explicitamente autorizado. Os resultados, ideias, parágrafos, ou outros extratos tomados de ou inspirados em trabalhos de outros autores, e demais referências bibliográficas usadas, são corretamente citados.

Autor - Luís Miguel Cunha Fernandes

Faculdade de Engenharia da Universidade do Porto

Resumo

A presente dissertação teve como objetivo desenvolver um sistema de identificação de objetos e pessoas para bancada laboratorial, sendo que para a identificação de objetos foi utilizada a tecnologia *Radio Frequency Identification* - RFID e para a identificação de pessoas a tecnologia *Near Field Communication* - NFC.

O trabalho desenvolvido teve como base um sistema de reservas das bancadas de laboratório, onde todos os utilizadores podem agendar as suas ações de trabalho. Deste modo, garante-se que todos os utilizadores definam horas para utilizarem as bancadas, evitando assim, esperas desnecessárias devido a estas se encontrarem ocupadas. O sistema de reservas também permite aceder ao histórico de utilizações de uma bancada e a execução de ações ao nível da administração do laboratório, como o registo de novos utilizadores ou de novas bancadas.

Cada bancada de laboratório foi equipada com um leitor da tecnologia NFC. Deste modo, para a execução de um trabalho numa bancada, cada utilizador identifica-se no leitor da bancada através de um *smartphone* que suporte a tecnologia (ou de um cartão NFC), sendo autorizado o seu trabalho se existir uma reserva prévia para a bancada associada ao utilizador em questão.

Durante uma ação de trabalho numa bancada, são registadas as horas de início e fim, bem como todos os objetos utilizados na execução de um trabalho. Os objetos mais comuns são frascos não metálicos com reagentes do tipo sólido ou líquido. Todos os objetos têm uma etiqueta RFID de modo a puderem ser identificados inequivocamente pelo leitor RFID da bancada.

Uma das vantagens deste trabalho, é que foi desenvolvido de acordo com uma arquitetura modular e extensível de modo a permitir que seja implementado em diversos laboratórios, independentemente número de bancadas. Além disso, os leitores NFC ou RFID em cada bancada podem ser substituídos, ou acrescentados, por outros de qualquer modelo ou marca , sem que haja necessidade de alterar a arquitetura do sistema.

O trabalho implementado possui também a capacidade de gerir algumas características da bancada, como por exemplo gavetas com fechaduras eletrónicas só se encontrarem acessíveis durante a utilização da bancada.

Em suma, esta dissertação culminou com um sistema de gestão de acesso a bancadas de laboratório, que permite uma otimização quer da utilização dos recursos, quer do tempo dos utilizadores, bem como com a criação de um histórico de utilizações para cada bancada laboratorial.

Abstract

The aim of the present dissertation was to develop a system for objects and people identification in a laboratory bench. To identify objects was used the technology Radio Frequency Identification -RFID and for people was used the technology Near Field Communication - NFC.

This work was developed based on a reservation bench system, where all users can schedule their work sessions. In order to ensure that, all users can define work hours in a bench, thus avoiding waiting because the bench was occupied. Furthermore, this reservation system allows access to a utilizations history and perform some laboratory administration actions, such as register new users or new benches in the system.

Each bench was equipped with a NFC reader. To work in a bench, each user will identify themselves with a NFC-enabled Smartphone or NFC card being only authorized to use the bench with a previous reservation.

During the work, the initial and the end hours of work are recorded in a database as well all objects used in the work. The most common objects are non-metallic flasks with reagents of solid or liquid nature. All objects have a RFID tag so the system can identify unequivocally the objects.

This work is extensible and can be implemented in different laboratories with different number of benches. Furthermore, this work was developed following a modular architecture allowing the addition or replacement of NFC or RFID readers of any brand or model without the necessity to change the system architecture.

The work also implements the capacity to manage some bench characteristics. For example having some electronic locked drawers only accessible during the work session.

In short, this master thesis culminated in a management system of access to laboratory benches, which allows an optimization of both the use of resources and the users time, as well the creation of a history of use for each laboratory bench.

Agradecimentos

O nosso sucesso profissional é tanto maior, quanto melhor for a nossa vida particular. Assim, quero agradecer a todos os que me proporcionaram bons momentos e que, muitas vezes sem saberem, ajudaram-me a ultrapassar situações menos agradáveis.

Quero agradecer ao Professor Paulo Portugal pelos conselhos acertados, ajuda e tempo investido na orientação da minha dissertação.

Ao professor Joaquim Gabriel pela disponibilidade e ajuda na clarificação dos requisitos necessários para o trabalho.

Aos meus professores que, de alguma forma, me ajudaram a crescer enquanto pessoa ao longo do meu percurso académico. Um obrigado especial aos professores Pedro Guedes de Oliveira e Luís Teixeira, por toda a disponibilidade demonstrada e pelos sábios conselhos dados.

À minha família. Ao meu pai que muitas vezes precisando de ajuda, sempre me incentivou a colocar a Faculdade em primeiro lugar. À minha mãe por toda a motivação e ajuda desde sempre. À minha irmã que me aturou, aguentou e ajudou sempre que precisei. Bem sei que muitas vezes sou duro com ela, mas é porque tenho a convicção que é a melhor maneira de a chamar à razão. À minha avó por toda a ternura e afeto que me deu. Ao meu avó pelo percurso público que fez, permitindo-me perceber e interessar pela causa pública.

À minha namorada. Companheira de tristezas e alegrias, sempre me incentivou e fez acreditar que valia a pena ficar a trabalhar mesmo quando toda uma cidade está em festa. Pode ter sido pouca animada, mas foi uma noite de S. João recheada de trabalho.

Aos meus amigos. A todos! Desde os amigos da "terrinha" que estão sempre dispostos a um café ao fim de semana ou a uma futebolada. Aos amigos da Faculdade (Porto, Coimbra e Žilina) que me proporcionaram momentos únicos e inesquecíveis. Um agradecimento especial ao *super guerreiro* César, ao Tiago, ao Lopes, ao Ricardo, ao Saleiro, ao Olhinhos, ao Zé e a todos os outros que muito contribuíram para o meu sucesso académico.

Miguel Fernandes

"O único lugar onde o sucesso vem antes do trabalho é no dicionário."

Albert Einstein

Conteúdo

Lista de Figuras

Lista de Tabelas

Abreviaturas e Símbolos

ASK	*Amplitude-shift Keying*
bps	bits por segundo
cm	centímetro(s)
CSS	*Cascading Style Sheets*
EEPROM	*Electrically Erasable Programmable Read-Only Memory*
UPC	*Universal Product Code*
FDX	*Full-duplex*
FEUP	Faculdade de Engenharia da Universidade do Porto
GB	Giga Byte(s)
HDMI	*High-Definition Multimedia Interface*
HDX	*Half-duplex*
HTML	*HyperText Markup Language*
I^2C	*Inter-Integrated Communication*
I/O	*input/output*
IP	*Internet Protocol*
kBit(s)	QuiloBit(s)
kByte(s)	QuiloByte(s)
kHz	Quilo-Hetz
LAMP	*Linux, Apache, MySQL e PHP*
MBit(s)	Megabit(s)
MHz	Mega-Hetz
ms	mili-segundo(s)
NFC	*Near Field Communication*
OCR	*Optical Character Recognition*
P2P	*peer-to-peer*
PHP	*Hypertext Preprocessor*
PIN	*Personal Identification Number*
RF	Radiofrequência
RFID	*Radio Frequency Identification*
SEQ	Sistemas Sequenciais
SQL	*Structured Query Language*
SRAM	Memória Estática de Acesso Aleatório
TCP	*Transmission Control Protocol*
UART	*Universal Asynchronous Receiver/Transmitter*
UPC	*Universal Product Code*
UEI	Unidade de Ensino e Investigação
UHF	Ultra Alta Frequência
UID	*Unique Identifier*
V	*Volt(s)*

Capítulo 1

Introdução

1.1 Enquadramento

No atual mercado global consumista, imerso em diferentes soluções capazes de responder aos nossos problemas, urge apostar na diferenciação tecnológica como meio de tornar os nossos produtos mais apetecíveis.

Assim, esta dissertação tem como objetivo otimizar a gestão de bancadas laboratoriais existentes em laboratórios [1], dotando-as de funcionalidades, úteis e práticas, que melhorem a experiência de trabalho dos colaboradores. Deste modo, pretende-se que os colaboradores dos laboratórios possam agendar todas as ações de trabalho e tenham a garantia de as puder executar nos momentos previamente definidos.

1.2 Motivação

A empresa LABORIAL tem "como core-business o fabrico, comercialização e instalação de mobiliário técnico laboratorial e hospitalar" [1], sendo reconhecida pelas soluções modernas que apresenta para a monitorização de laboratórios.

Esta dissertação, foi desenvolvida no âmbito do projeto INTELLAB e realizada na FEUP, em pareceria com a empresa LABORIAL, com o intuito de identificar quais as pessoas e quais os objetos utilizados nas bancadas laboratoriais existentes nos seguintes laboratórios: anatomia patológica, fabrico de injetáveis, segurança biológica P1 a P4, veterinários ou de experimentação animal.

1.3 Objetivos

Pretende-se que seja desenvolvido um sistema de gestão de acessos a bancadas de laboratório, tendo como característica chave o agendamento de reservas por parte dos colaboradores. Deste modo, cada bancada será utilizada em horas pré-definidas, permitindo a otimização, quer do tempo

[1] Ambiente de laboratório descrito em 2.1

dos colaboradores, quer da utilização das bancadas, possibilitando assim um aproveitamento mais eficiente dos recursos.

Além da gestão de reservas, esta dissertação tem também como objetivos a identificação de objetos e de pessoas que utilizam as bancadas laboratoriais. Para a identificação de objetos será utilizada a tecnologia RFID, recorrendo para isso a um leitor e a etiquetas RFID. Pretende-se assim, saber quais foram os objetos utilizados pelo colaborador para efetuar um dado trabalho. A identificação de pessoas, depende das especificações de cada ambiente de trabalho e poderá ser efetuada de duas formas distintas, sendo elas: com recurso a cartões NFC ou então, *smartphones* que suportem a tecnologia NFC.

O desenvolvimento desta dissertação tem também a característica das tecnologias a incorporar na bancada de laboratório serem modulares, isto é, permitir que os leitores possam ser substituídos por outros, independentemente do fabricante. Esta questão é um fator bastante importante, pois permite que os sistemas de identificação possam ser atualizados por outros do mesmo tipo.

As reservas de bancadas, bem como o registo da informação recolhida pelos dispositivos incorporados na bancada, serão geridos por uma interface web que interagirá com uma base de dados. A interface web será intuitiva, permitindo deste modo uma utilização rápida e eficaz por parte dos colaboradores.

Assim, esta dissertação tem como objetivos:

- criação de sistema de agendamento para reserva das bancadas laboratoriais.
- identificação de objetos com recurso a etiquetas RFID.
- identificação de pessoas através da tecnologia NFC.
- implementação de interface web, com ligação a uma base de dados, para registo de novos utilizadores, novas bancadas ou novos objetos no laboratório, bem como criação e visualização de histórico de utilizações das bancadas.

1.4 Estrutura da Dissertação

O presente documento encontra-se organizado em 5 capítulos.

No capítulo 1 encontram-se descritos o enquadramento, a motivação, os objetos e a estrutura desta dissertação.

No capítulo 2, é feita a caraterização do ambiente de trabalho em laboratórios, sendo também apresentadas tecnologias de identificação e recolha de dados automáticos, com maior ênfase nas tecnologias RFID e NFC, porque foram as utilizadas no desenvolvimento desta dissertação.

No capítulo 3, designado arquitetura do sistema, é apresentada uma análise de requisitos do sistema, bem como descrita a arquitetura que se desenvolveu para a conceção do trabalho proposto.

No capítulo 4 são abordadas as características técnicas do *hardware* utilizado e são também descritos os passos efetuados na implementação do sistema de gestão de acessos às bancadas de laboratório.

Por fim, no capítulo 5 apresentam-se as principais conclusões da dissertação realizada, bem como sugestões para possíveis trabalhos futuros.

Capítulo 2

Ambiente em laboratório e descrição de tecnologias de identificação automática

No presente capítulo, será caracterizado o ambiente onde a bancada de laboratório será inserida. Serão também apresentadas as características das tecnologias a serem incorporadas na bancada, nomeadamente as tecnologias RFID e NFC.

2.1 Caracterização de laboratórios

Uma bancada de laboratório é um espaço com características próprias, nomeadamente ao nível das caraterísticas físicas dos materiais que a constituem, de modo a que se possam utilizar para a realização de um dado trabalho e que sejam facilmente desinfetadas. Por esta razão, as bancadas de laboratório são constituídas por superfícies lisas e planas, facilitando assim a sua limpeza.

Os laboratórios têm na sua constituição, entre outras coisas, bancadas de laboratório e possuem, por norma, regulamentos específicos de funcionamento onde são definidas as regras básicas de segurança. Desde os laboratórios de anatomia patológica, passando pelos laboratórios de fabrico de injetáveis, pelos laboratórios de segurança biológica P1 a P4, até aos laboratórios veterinários ou de experimentação animal, existe um conjunto de normas distintas de acordo com o tipo de trabalho desenvolvido em cada um deles.

De acordo com o Manual de Segurança Biológico do Instituto de Higiene e Medicina Tropical da Universidade Nova de Lisboa [2], algumas das normas dos laboratórios de segurança biológica P1 e P2 são:

- Acesso à zona de trabalho condicionado a pessoal autorizado.
- Proibição de utilizar qualquer dependência que não seja a do laboratório em que se encontra a trabalhar, sem autorização do Diretor da Unidade de Ensino e Investigação - UEI.
- Proibição da entrada a crianças nas áreas de trabalho do laboratório.
- Proibição de comer, beber, fumar, maquilhar, guardar alimentos, bebidas ou objetos pessoais em qualquer parte do laboratório.
- Proibição de beber água da canalização do laboratório.

- Utilização de equipamento de proteção pessoal adequado no interior do laboratório, o qual deve ser removido antes de sair do laboratório. No mínimo, é obrigatório o uso de bata branca no laboratório.

2.1.1 Exemplos de bancadas de laboratório

De seguida, serão apresentados dois modelos distintos de bancadas de laboratório desenvolvidos pela Laborial, sendo que ambas as bancadas foram "desenvolvidas e testadas de acordo com a norma EN13150:2001". [3]

2.1.1.1 Linha Blau

A linha Blau, que se pode observar na figura 2.1, ilustra um tipo de bancadas de laboratório que se caracterizam por uma superfície plana com um "revestimento extremamente resistente a ambientes quimicamente agressivos" [3], tendo também uma zona de arrumação fechada na parte inferior da bancada e uma zona de tomadas, a vermelho, numa coluna vertical, tal como se pode observar na figura referida.

Figura 2.1: Imagem ilustrativa da integração da linha Blau em laboratório com 4 zonas de trabalho em primeiro plano [4]

2.1.1.2 Linha Ahmar

A linha Ahmar, ilustrada na figura 2.2, é uma bancada de laboratório "onde se realizam ensaios de elevada dureza e risco" e "está certificada segundo a norma EN 14175:2003 – Hotte de

química". [5] Este tipo de bancadas de laboratório, têm uma zona de arrumação na parte inferior da bancada, uma janela na parte superior que, caso esteja fechada, impede o acesso à superfície da bancada, e um sistema de extração de ar para evitar a inalação de vapores tóxicos provenientes do manuseamento de substâncias químicas na hotte.

Figura 2.2: Imagem ilustrativa da linha Ahmar [6]

2.2 Tecnologias de Identificação Automática

A experiência já vivida pelos nossos antepassados leva-nos inequivocamente a concluir que, em qualquer tipo de trabalho, este é tanto mais rentável quanto mais facilmente estiverem à nossa disposição as matéria-primas e/ou os utensílios de trabalho, que serão necessários à sua realização. Neste contexto, é natural que uma grande gama de industrias como: produção, transformação, transporte, distribuição, até às industrias de comercialização ao consumidor final, pretendam ter um controlo eficaz da gestão dos seus recursos.

Um sistema de controlo eficaz a ser implementado, tem de ser capaz de identificar inequivocamente, consoante o objetivo em questão claro, o objeto, material ou a pessoa pretendida. Ou seja,

qualquer que seja o sistema a adotar, este tem de ser suficientemente robusto a todas as adversidades do meio em que irá ser instalado, bem como ser capaz de identificar o que seja pretendido de forma eficiente.

A instalação de sistemas de controlo de pessoas, permite ainda uma maior responsabilização por parte de quem utiliza os recursos em questão, pois como estes podem detetar quem os está a manusear, pode-se identificar de forma transparente qual o utilizador que causou um determinado dano num recurso podendo-se, por exemplo, responsabilizar-se quem de direito no caso de utilizações inapropriadas.

Os sistemas de identificação e recolha de dados automáticos, também comummente denominados sistemas de identificação automática, assumem-se como excelentes soluções para resolver os problemas supra-referidos, porque têm como objetivo identificar, monitorizar e recolher eventuais dados associados a objetos ou pessoas, de forma totalmente autónoma e com um grau de fiabilidade elevado.

No nosso dia-a-dia e, possivelmente sem nos apercebemos, estamos em contacto com tecnologias de identificação automática. Por exemplo, numa ida a um hipermercado podemos tomar contacto com a tecnologia de código de barras que é utilizada para registar os produtos qe pretendemos adquirir, utilizar a tecnologia de banda magnética ao pagar a conta com o cartão bancário e ainda recorrer a um sistema RFID, caso se passe por alguma portagem do tipo Via Verde.

Em suma, as tecnologias de identificação automática estão muito presentes numa vasta gama de sectores de atividade e existem para fornecerem informação sobre pessoas, animais, objetos ou produtos, quer estejam em movimento, ou na ausência deste. [7]

2.2.1 Tecnologias para os sistemas de identificação

Atualmente existem diversas tecnologias de identificação automática. Cada uma delas possui características próprias e específicas, o que se traduz em soluções com vantagens e desvantagens diferentes para cada uma das tecnologias. Assim sendo, uma tecnologia pode-se revelar excelente para desempenhar uma dada função A, mas pode ser pouco eficaz para uma aplicação numa opção B.

As tecnologias de identificação automática mais importantes existentes atualmente são: reconhecimento ótico de carateres, código de barras, RFID e NFC, smart cards e biometria, tal como se pode observar na 2.3.[7] Todas as tecnologias referidas foram desenvolvidas com objetivos específicos, tendo ambas como filosofia a identificação e recolha de dados sem intervenção humana.

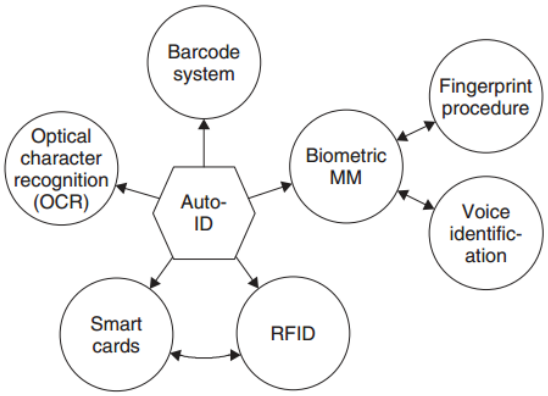


Figura 2.3: Tecnologias de identificação automática mais importantes [7]

De seguida, serão apresentadas as tecnologias acima enumeradas, sendo que a primeira a ser abordada é o reconhecimento ótico de caracteres - OCR.

2.2.1.1 OCR - Reconhecimento Ótico de Carateres

O OCR é uma tecnologia que foi utilizada pela primeira vez nos anos 60, que converte imagens de texto para documentos editáveis em computadores. Nos casos em que ocorram falhas na deteção de caracteres, o sistema OCR passa-os à frente, originando erros.

A tecnologia OCR foi desenvolvida de modo a que pudesse ser utilizada de forma automática por máquinas (figura 2.4) ou de forma manual por pessoas (figura 2.5). A utilização deste tipo de sistemas está basicamente confinada para a execução de serviços administrativos, bem como para o registo de cheques em bancos.

Segundo [7], a principal vantagem dos sistemas OCR é a alta densidade de informação. Outra vantagem deste tipo de sistemas é que permitem reduzir a quantidade de papel a armazenar numa empresa e, simultaneamente, facilitam a organização, ou edição de documentos, visto que estes passam a ser guardados em formato digital.

Contudo, os sistemas OCR não conseguiram singrar como poderiam a nível universal devido ao seu elevado preço em relação a outras soluções concorrentes. Outras desvantagens desta tecnologia eram a quantidade de erros que surgiam durante o reconhecimento de um texto, podendo estes dever-se a um baixo contraste entre o texto e o seu fundo, ou então, devido ao facto do documento possuir texto e imagens. Em qualquer dos casos, a utilização dos sistemas OCR "obrigava" a uma revisão manual integral do texto obtido, comparando-o com o texto original, o que originava um trabalho demoroso, tornando a tecnologia pouco apelativa para ser utilizada no reconhecimentos de textos extensos. [7]

Figura 2.4: Leitor automático de reconhecimento ótico de carateres [8]

Figura 2.5: Leitor manual de reconhecimento ótico de carateres [9]

2.2.1.2 Código de Barras

A tecnologia de código de barras permite a representação gráfica de dados, quer numéricos, quer alfanuméricos. Esta tecnologia tem duas variantes: códigos de barras lineares e códigos de barras a duas dimensões que podem ser observadas, respetivamente, na figura 2.6.

Figura 2.6: Exemplos de diferentes tipos de códigos de barras [10]

Os códigos de barras lineares, também denominados unidimensionais, são constituídos por uma sequência de barras pretas e brancas, que são lidas num sentido. Por sua vez os códigos de barras a duas dimensões, também designados bidimensionais, são compostos por informação codificada armazenada em linhas e colunas, podendo serem lidos em qualquer posição. Em alguns casos, os códigos de barras bidimensionais possuem sistemas de redundância (até 40 %), podendo assim serem descodificados mesmo que estejam parcialmente danificados. [11]

Nesta tecnologia, a informação é codificada através da variação do tamanho ou da forma das barras pretas, bem como a distância entre elas. A informação codificada nos códigos de barras pode ser descodificada através de qualquer dispositivo capaz de ler a imagem, como por exemplo, leitores de códigos de barras ou *smartphones*.

Os tipos de códigos de barras mais comuns são os *European Article Number - EAN* que representam uma evolução dos códigos de barras *Universal Product Code*, originários nos Estados Unidos da América. Os códigos EAN são constituídos por 13 dígitos: o identificador do país, o identificador da empresa, número de artigo do fabricante e um dígito de verificação, tal como se pode observar na figura 2.7.

Figura 2.7: Exemplo de código de barras EAN [12]

De modo sucinto, as vantagens dos códigos de barras são a sua fácil e barata produção, a facilidade de leitura, o seu longo tempo de vida, a menos que sofra alguma dano, bem como a sua ampla aplicação e a sua leitura rápida. Por outro lado, as suas principais desvantagens são a necessidade de contacto visual entre o código e o leitor, o facto de não possibilitar a sua escrita, nem poderem ser lidos em simultâneo e a sua baixa segurança. [7]

Os códigos de barras bidimensionais têm vindo a ganhar mercado nos últimos anos, sendo que existem diversos tipos destes códigos, tal como se pode observar na figura 2.8. O tipo de códigos de barras bidimensional mais conhecido é o QR code, sendo muito utilizado nas áreas do marketing e da comunicação, permitindo, por exemplo, uma ligação entre a comunicação *offline* através da publicidade, com a comunicação *online*, no caso do código de barra bidimensional nos reencaminhar para uma página web.

Figura 2.8: Exemplos de códigos de barras bidimensionais [11]

Na figura 2.9, pode-se observar uma aplicação prática dos QR codes numa iniciativa lançada pela Associação de Valorização do Chiado, apoiada pelo Turismo de Portugal. O objetivo da iniciativa em questão é fornecer informações sobre a calçada portuguesa aos turistas, assumindo-se como o primeiro QR code no mundo feito em calçada portuguesa. [13] [14]

Figura 2.9: Qr code em calçada portuguesa no Chiado - Lisboa [15]

2.2.1.3 *Smart Cards*

Um *smart cards*, em português denominado cartão inteligente, é um sistema eletrónico de armazenamento de dados que pode ter, eventualmente, capacidade computacional através de um microprocessador. Este tipo de tecnologia, tem diversas aplicações, tais como cartões de telemóveis, cartões de crédito, cartões de identificação para acesso, entre outro. Por questões meramente de conveniência, é usual que os *smart cards* sejam incorporados em cartões de plástico do tamanho de um cartão de crédito.

De acordo com as suas características internas, os *smart cards* podem-se dividir em dois subgrupos: os cartões de memórias e os cartões com microprocessador onde, os primeiros, têm apenas a capacidade de armazenamento de dados, ao passo que os segundos têm capacidade computacional.

De forma genérica, para o funcionamento dos *smart cards* é necessário um leitor que efetua uma conexão elétrica com as superfícies dos contactos galvânicos do cartão inteligente, com recurso a molas de contacto que forneceram energia ao cartão inteligente, bem como estabeleceram um sinal de relógio necessário à leitura e transferência de dados, bidirecional, entre o *smart card* e o leitor.

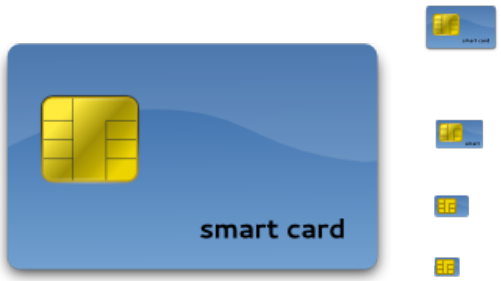


Figura 2.10: Ilustração de vários tipos de cartões inteligentes[16]

Os *smart cards* têm como principais vantagens a possibilidade de proteção contra acessos indesejados e também contra a manipulação da informação que contêm. Esta proteção é assegurada através de um número de identificação pessoal, vulgarmente designado código PIN - *Personal Identification Number* . Por estes motivos, os cartões inteligentes são muito utilizados em transações financeiras, tornando-as simples, seguras e baratas do ponto de vista operacional. No entanto, os cartões inteligentes têm como principais desvantagens a sua cara manutenção e o desgaste dos contactos, fenómenos de corrosão ou ainda a existência de pó que pode tornar inoperacional a comunicação através dos contactos. Na figura 2.10, pode-se observar de forma clara os contactos referidos, que aparecem na figura a amarelo.

Figura 2.11: Ilustração de leitor de cartões inteligentes [17]

De acordo com [7], no ano de 1992 foram emitidos em todo o mundo cerca de 200 milhões de cartões inteligentes e no ano de 1995, este número cresceu para os 600 milhões, dos quais 500 milhões eram cartões de memória e 100 milhões eram cartões com microprocessador.

2.2.1.4 Biometria

A palavra Biometria resulta da conjunção de duas palavras gregas: *bios*, que significa vida, com a palavra *metron* que significa medida. [18] A tecnologia que tem por base a Biometria recorre às propriedades físicas, biológicas e únicas dos seres vivos para a sua identificação, pelo que não pode ser utilizada em objetos.

Normalmente, esta tecnologia é utilizada para a identificação de pessoas, através das suas caraterísticas físicas individuais e inconfundíveis, isto é, recorre-se, a caraterísticas biométricas biológicas ou características comportamentais, por forma a identificar uma pessoa. Como caraterísticas biométricas biológicas mais utilizadas temos as impressões digitais, a íris dos olhos ou o reconhecimento facial; como características comportamentais temos os manuscritos, a identificação por voz ou ainda padrões na utilização de teclados.

Analisando o funcionamento do processo da identificação por voz, por exemplo, ver-se-á que este se baseia na captação da voz de uma determinada pessoa que fala para um microfone ligado a um sistema com capacidade computacional e este, recorrendo à conversão da voz em sinais digitais, que comparará os sinais digitais recebidos com sinais previamente guardados num software de identificação por voz, verificando a sua identidade. Posteriormente, e caso a identidade da pessoa seja conhecida, pode desencadear uma determinada ação como a abertura de portas.

As grandes vantagens dos sistemas de identificação por biometria são a sua segurança e a sua conveniência. Com este tipo de sistemas, deixa de haver, por exemplo, custo económicos associados a perdas de cartões de identificação. Contudo existe ainda ressalvas a fazer por causa das fraudes. Neste sentido, por exemplo, os sistemas de impressão digital de identificação evoluíram por forma detetar se o dedo colocado sobre o leitor pertence, ou não, ao de uma pessoa viva. [7]

De acordo com a SINFIC [19], os sistemas biométricos podem ser utilizados, paralelamente ao seu uso convencional, para a deteção de fraudes. A referida fonte refere o exemplo uma "pessoa que opte por se identificar perante um sistema com o dedo indicador direito e/ou com a leitura do olho direito", poderá no contexto de uma tentativa de intrusão ilícita, colocar o dedo indiciador esquerdo e/ou mostrando o olho esquerdo para leitura, tendo assim oportunidade de alertar o sistema da potencial fraude. Ainda citando a mesma fonte, "claro que as amputações também são possíveis, mas a conjugação de vários dados biométricos tornará os sistemas quase invioláveis, embora também diminua a conveniência referida atrás."

2.2.1.5 RFID

Atualmente, os sistemas RFID, em português também designados sistemas de identificação por radiofrequência - RF, podem-se relacionar com os *smart cards* porque ambos armazenam os dados num dispositivo eletrónico - o *transponder*. Uma das grandes diferenças entre os dois

sistemas prende-se ao nível do fornecimento de energia pois os sistemas RFID funcionam com recurso a leitores que alimentam as etiquetas, através da utilização de campos magnéticos ou eletromagnéticos, em detrimento da utilização de contactos elétricos dos cartões inteligentes. [7]

A tecnologia RFID tem como características o armazenamento, leitura, gravação e manipulação de dados em etiquetas RFID através da comunicação com os leitores RFID. [7] Quando uma etiqueta RFID está numa zona de leitura de um leitor RFID, este é capaz de comunicar com a etiqueta através de campos magnéticos ou eletromagnéticos, conseguindo ler a informação que a etiqueta RFID possui. Dependendo das características do leitor RFID, pode-se conseguir efetuar a leitura simultânea de diferentes etiquetas RFID presente na zona de leitura de um leitor.

Figura 2.12: Leitor e etiqueta RFID [20]

Nos últimos anos a tecnologia RFID tem vindo a disseminar-se nos mercados devido às enumeras vantagens que estes sistemas apresentam: ausência da necessidade de contacto, grande fiabilidade, possibilidade de guardar informações, bem como dificuldades em modificar a informação guardada.

2.2.2 Análise comparativa

Na tabela 2.1 pode-se observar uma comparação entre as várias tecnologias.

Tabela 2.1: Tabela comparativa - Tecnologias de Identificação Automática enunciadas [7]

Característica	**OCR**	**Código de Barras**	***Smart Cards***	**Biometria**	**RFID**
Volume de dados armazenados	1-100 Bytes	1-100 Bytes	16-64 KBytes	-	16-64 KBytes
Densidade de dados	Baixa	Baixa	Muito Elevada	Elevada	Muito Elevada
Leitura - dispositivos de leitura	Boa	Boa	Boa	Cara	Boa
Leitura - por pessoas	Simples	Limitada	Impossível	Difícil	Impossível
Influência de humidade e poeiras	Muito Elevada	Muito Elevada	Possível [1]	-	Sem influência
Influência de cobertura da tecnologia	Falha total	Falha Total	-	Possível	Sem influência
Influência da direção e posição	Baixa	Baixa	Unidirecional	-	Sem influência
Degradação	Limitada	Limitada	Contactos	-	Sem influência
Custos de aquisição	Médios	Muito Baixos	Baixos	Muito Altos	Médios
Custos de operação	Baixos	Baixos	Médios [1]	Nenhum	Nenhum
Cópia/modificação não autorizada	Leve	Leve	Impossível	Impossível	Impossível
Velocidade de leitura [2]	Baixa 4s	Baixa 3s	Baixa 4s	Muito Baixa >5ms	Muito rápida 0,5s
Distância máxima de leitura	<1 cm leitor	0-50cm	Contacto direto	Contacto direto [3]	0-5m

Após uma análise da tabela 2.1, e de acordo com as características acima descritas do ambiente em laboratório, proceder-se-á à seleção das tecnologias para identificação de pessoas e objetos para fim de identificação. De notar que todos os sistemas foram criados com especificidades próprias e não para se substituir uns aos outros, sendo assim, naturalmente, alguns acabam por satisfazer melhor os requisitos em que se enquadra o projeto.

Começando pelas tecnologias de códigos de barras e de reconhecimento ótico de caracteres, estas revelam desde logo um problema: o ambiente em laboratório pode ser muito adverso pois existe a necessidade de limpeza associada aos objetos que são utilizados. A limpeza contínua dos objetos em que poderão estar os códigos de barras, ou o contacto com substâncias que possam, por exemplo, deteriorar uma parte do código, levando à sua deformação e tornando-os inoperacionais. Deste modo, as tecnologias a utilizar para a identificação de objetos devem ser robustas a esta característica.

Por seu turno, os *smart cards* revelam-se também pouco adaptados ao uso pretendido pelo facto de existirem apenas em formato de cartão, que necessita de contacto físico com o leitor, o que não permite, por exemplo, a identificação simultânea de vários objetos.

Por fim, as tecnologias que melhor se adaptam aos requisitos do problema são o RFID para a identificação de pessoas e objetos e a biometria, apenas para a identificação de pessoas. Por questões meramente optativas, escolheu-se utilizar a tecnologia RFID no desenvolvimento do trabalho.

2.3 RFID - Identificação por Rádio Frequência

2.3.1 A origem do RFID

A tecnologia RFID teve o seu prelúdio durante a Segunda Guerra Mundial. Na altura, o objetivo prendia-se com a necessidade de saber se o avião que se estava a aproximar era um avião aliado ou um avião inimigo porque, através do recurso a radares, os exércitos conseguiam apenas detetar a aproximação de um avião. No decorrer da Guerra os alemães descobriram que se os aviões que estivessem de regresso à base girassem, a onda detetada pelos radares era alterada, conseguindo assim interpretar a presença da aviões como seus conhecidos. Na verdade, este foi considerado o primeiro sistema passivo de RFID.

Por seu turno, os ingleses levaram a cabo o desenvolvimento de um sistema que permitiu o nascimento dos identificadores ativos. Neste sistema, era colocado um transmissor em cada avião, que quando recebiam sinais dos radares, emitiam um sinal de resposta, identificando assim o avião como conhecido. Claro está, que se fosse detetado um avião nas proximidades e não existisse sinal de resposta, tratar-se-ia de um avião inimigo.

O funcionamento atual dos sistemas RFID, assenta numa filosofia muito semelhante pois existe um leitor que envia um sinal para uma etiqueta RFID e esta etiqueta recebe o sinal, posteriormente

[1] Contactos.

[2] Entre o leitor e componente a ser lido.

[3] No caso da identificação por impressão digital. A identificação através da íris, ou por reconhecimento de voz, não necessita de contacto direto.

ou reflete o sinal de volta (sistema passivo), ou transmite um sinal de resposta próprio (sistema ativo).

Até aos anos 70 e, apesar dos avanços na área dos radares e de comunicação RF, os sistemas RFID eram apenas restritos ao uso militar, nomeadamente para se garantir a segurança de locais críticos, como por exemplo locais com tecnologia nuclear. No final dos anos 70 a tecnologia RFID chegou ao setor privado, tendo sido uma das primeira utilizações do sistema a aplicação da tecnologia para identificação de gado bovino na Europa. [21]

Durante a década de 80 a tecnologia continuou a sofrer avanços, nomeadamente no campo das etiquetas passivas, sendo que em 1990 começou-se a normalização dos sistemas RFID e esta tecnologia continuou o seu percurso de evolução, ganhando maturidade até aos dias de hoje. [21] [22]

2.3.2 Descrição sumária

O RFID é uma tecnologia que tem como princípio a identificação por RF. Para que a identificação de um dado objeto seja possível recorremos a etiquetas RFID, que, quando colocadas na presença de um leitor, estabelecem uma conexão via RF com este, permitindo a leitura e/ou a escrita na etiqueta RFID, consoante o tipo de etiqueta em questão. De modo a tratar a informação obtida por um leitor RFID convenientemente, estes podem ser ligados, por exemplo, a computadores para processamento dos dados adquiridos.

Deste modo, tal como se pode observar na figura 2.13 pode-se decompor os sistemas RFID em dois componentes:

- a etiqueta RFID: a colocar no objeto a ser identificado;
- o leitor: que pode ler/escrever nas etiquetas RFID.

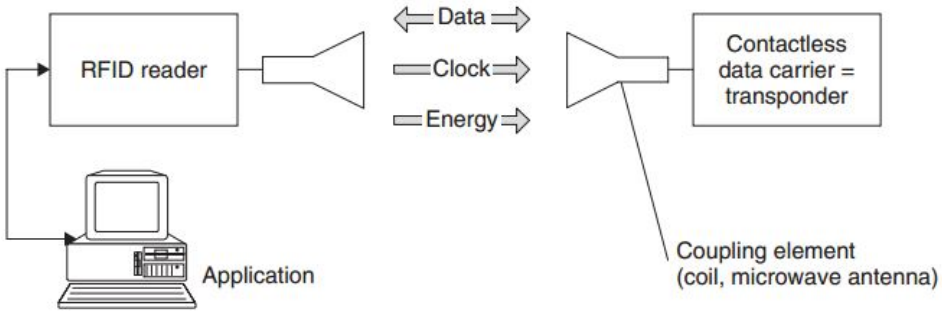


Figura 2.13: Componentes de sistemas RFID [7]

2.3.3 Modos de comunicação

O funcionamento de sistemas RFID assenta na lógica da leitura de etiquetas RFID por parte de leitores RFID. Os leitores RFID, quando se encontram ligados, conseguem detetar etiquetas numa zona periférica do leitor, designada como zona de interrogação do leitor RFID. Esta zona pode-se

então definir como a área envolvente ao leitor onde a potência do campo eletromagnético por ele criado é suficiente para a comunicação com etiquetas RFID. Quando uma etiqueta está presente na referida zona de interrogação, esta pode ser lida e/ou escrita pelo leitor porque o *transponder* é ativado; ao passo que quando a etiqueta não está na zona de interrogação de um leitor esta não pode ser lida nem escrita pelo leitor.

Os sistemas RFID podem operar de acordo com um de dois procedimentos: em *full-duplex*/ half-duplex ou sistemas sequenciais - SEQ. [23]

O modo *full-duplex - FDX* caracteriza-se pela transferência de dados entre a etiqueta RFID e o leitor acontecer simultaneamente com a transferência de dados entre o leitor e a etiqueta RFID. Para o fluxo de dados ocorrer ao mesmo tempo, são transmitidos dados em frequências diferentes, com recurso a sub-harmónicos ou a outras frequências. Este modo é bastante utilizado com etiquetas RFID ativas.

No modo de operação *half-duplex - HDX*, a transferência de dados entre o leitor e a etiqueta RFID ocorrem alternadamente com a transferência de dados entre a etiqueta RFID e o leitor. Este processo, característico de etiquetas RFID do tipo passivas, é utilizado quer em frequências abaixo dos 30 MHz onde se recorre à modelação *amplitude-shift keying* - ASK, com ou sem sub-portadora, quer em frequências na gama dos 100 MHz, onde de recorre à tecnologia de radar. [24]

Em relação aos SEQ, estes caraterizam-se por operarem com uma interrupção do campo eletromagnético fornecido pelo leitor, o que não acontecia anteriormente. Posto isto, aquando da presença do campo eletromagnético, o leitor transfere dados para o *transponder*. A transferência de dados do *transponder* para o leitor ocorre na ausência do campo eletromagnético. Para que isto seja possível, as etiquetas que operam neste modo possuem condensadores que são carregados na presença do campo eletromagnético, através de energia induzida na antena, ou então recorrendo a baterias auxiliares, fornecendo assim a alimentação à etiqueta RFID durante a transmissão de dados para o leitor RFID. Devido à sua forma de funcionamento, diz-se que se trata de um sistema pulsado.

Na figura 2.14, é possível observar uma representação esquemática dos procedimentos supra referidos.

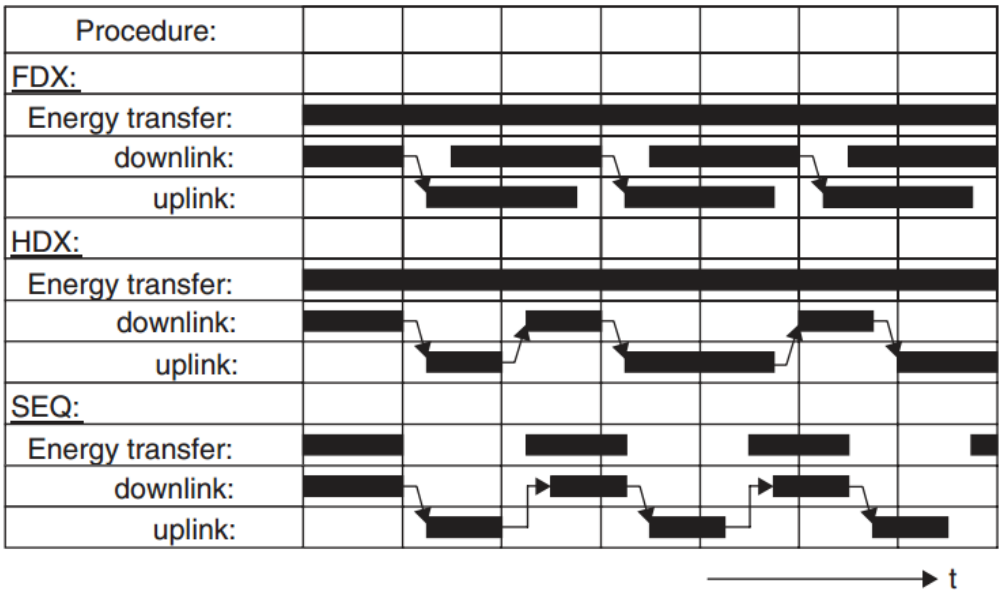


Figura 2.14: Tipos de procedimentos para a transmissão de dados usando a tecnologia RFID [7]

2.3.4 Frequência, Alcance e Acoplamento

Os sistemas RFID podem diferenciar-se, de forma sucinta, através de três critérios base: frequência de funcionamento do leitor, alcance do sistema e método de acoplamento. Os sistemas de RFID operam em frequências muito distintas que vão desde os 135 Khz até aos 5.8GHz (faixa de micro-ondas).

Ao nível de acoplamento físico são utilizados campos elétricos, magnéticos e eletromagnéticos, sendo que se conseguem alcances entre poucos milímetros até cerca de 15 metros. [7] Tal como se pode observar na fig 2.15, o tipo de acoplamento que atinge menores distâncias de comunicação é o acoplamento indutivo, onde as etiquetas RFID utilizam o campo magnético criado pelo leitor RFID para comunicar com este. Por outro lado, quando o acoplamento das etiquetas RFID é feito através de campos eletromagnéticos, conseguem-se alcançar maiores distâncias. Neste tipo de acoplamento, se o leitor for direcional conseguem-se criar maiores zonas de interrogação do que com leitores não-direcionais, pois a potência do campo criado é toda concentrada num dado sentido. No entanto, nestes casos, a posição da etiqueta em relação ao leitor tem de respeitar a direção do campo eletromagnético criado pois, caso contrário, a etiqueta não estará numa zona de leitura do leitor.

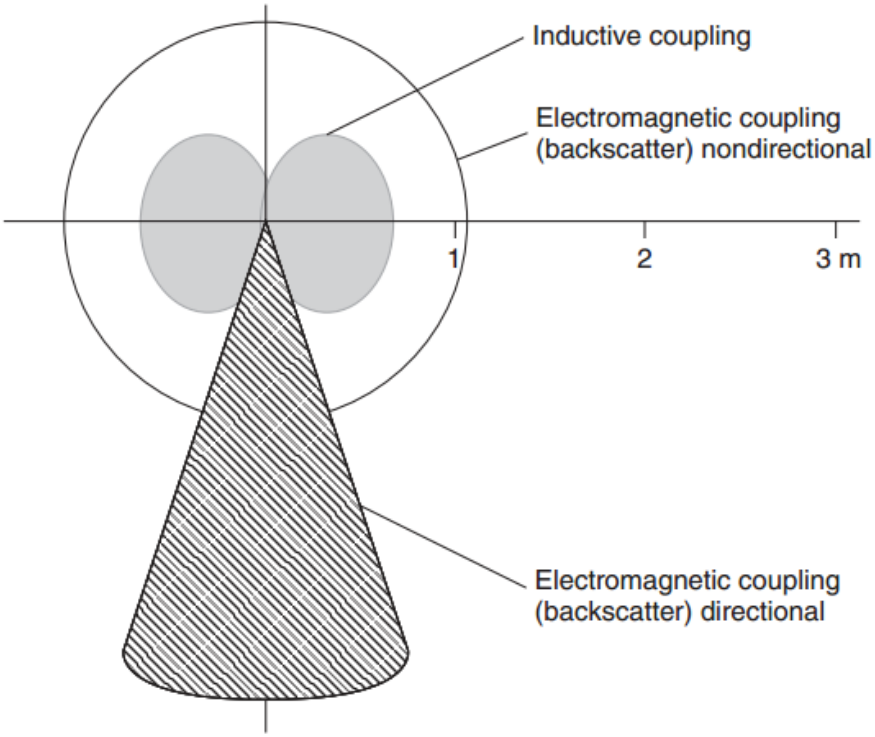


Figura 2.15: Comparação das zonas de interrogação para diferentes tipo de acoplamento [7]

Os sistemas RFID que têm um intervalo de comunicação até 1 cm, são denominados como *close-coupling systems* e têm vindo a perder mercado progressivamente. [7] Neste tipo de sistemas, a etiqueta RFID pode ser inserida no leitor RFID ou colocada sobre uma superfície de leitura prevista para o efeito de modo a ser efetuada a sua leitura, sendo que na comunicação entre o leitor e a etiqueta RFID são utilizados campos elétricos e magnéticos que podem operar com frequências até 30 MHz. Este tipo de sistemas são bastante utilizados em aplicações como portas de bloqueio automático ou sistemas de cartões inteligentes sem contacto com funções de pagamento.

No caso de sistemas RFID que conseguem ler e escrever com alcances até 1 metro, estes são denominados sistemas de acoplamento remotos. Regra geral, este tipo de sistemas utilizam um acoplamento indutivo entre o leitor e a etiqueta RFID sendo por este motivo também designados sistemas de rádio indutivos. De acordo com [7], cerca de 90% dos sistemas RFID vendidos atualmente utilizam um acoplamento indutivo.

Por fim, os sistemas RFID com intervalos acima de 1 metro até cerca de 15 metros, são chamados de sistemas de longo alcance ou sistema *backscatter*, porque as etiquetas RFID efetuam a retro-difusão das ondas eletromagnéticas do leitor para o envio de dados para o leitor. Todos os sistemas deste tipo comunicam com recurso a ondas RF, na faixa das ultra altas frequências ou de micro-ondas. Este tipo de sistemas, quando operam nas frequências UHF na Europa operam a 868 Mhz, ao passo que nos Estados Unidos da América operam a 915 MHz. As frequências de micro-ondas operam desde os 2.5 GHz até ao 5.8 Ghz. Regra geral, as etiquetas RFID dos sistemas de

longo alcance que operam com alcances até cerca 3 metros não possuem bateria, ao passo que as etiquetas RFID dos sistemas de longo alcance que operam entre os 3 até aos 15 metros utilizam baterias auxiliares. De salientar que a baterias dos *transponders* fornecem apenas energia para fazer funcionar o micro-chip e para o armazenamento de dados, sendo que a energia utilizada para a transmissão de dados é a induzida na antena através da potência do campo eletromagnético do leitor. [7]

2.3.5 Etiquetas RFID

Quando surgiram no mercado, as etiquetas RFID tinham como intuito substituírem os códigos de barras devido às vantagens que apresentam. Com a utilização destas etiquetas é possível a identificação dos produtos a alguma distância relativamente ao leitor, sendo que também não obriga ao alinhamento do leitor com a etiquetas, em detrimento do que acontece nos códigos de barras.

As etiquetas RFID são *transponders* que contém um circuito integrado e uma antena capazes de responder a sinais de rádio previamente enviados por uma antena emissora. Estas, são objetos de pequenas dimensões que podem ser colocadas em pessoas, animais, equipamentos, produtos, embalagens, entre outras coisas.

Na figura 2.16 pode-se observar dois *layouts* de etiquetas RFID. À esquerda, é visível uma representação esquemática de uma etiqueta RFID em que um *transponder* indutivo está acoplado a uma bobine de antena; e à direita, está ilustrada uma representação esquemática de um *transponder* de micro-ondas acoplado a uma antena dipolar.

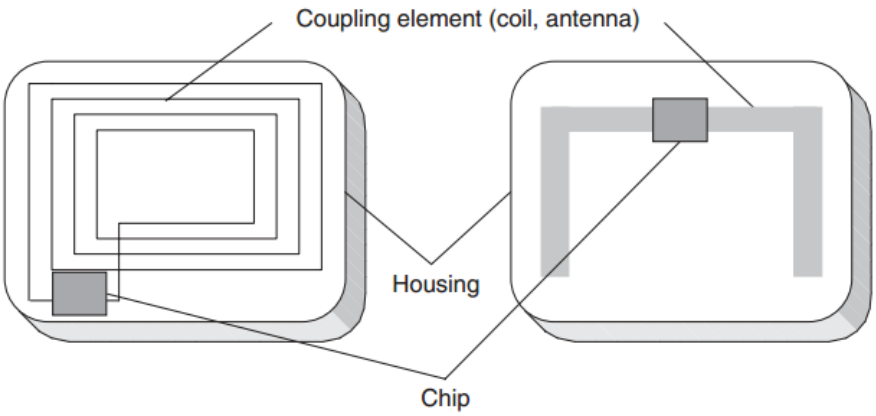


Figura 2.16: Ilustração de dois tipos *transponders* [7]

2.3.5.1 Frequências de Operação

As etiquetas RFID podem operar em 4 frequências distintas: baixa frequência, alta frequência, frequência ultra alta e micro-ondas. Normalmente, os sistemas RFID que utilizam frequências entre os 100 KHz e os 30 MHz, operam utilizando um acoplamento indutivo através do campo mag-

nético criado pelo leitor, ao passo que que os sistemas RFID que operam na gama de frequências de micro-ondas (2.45-5.8 GHz) utilizam um acoplamento através de campos eletromagnéticos.[7]

De acordo com [7], os sistemas RF de baixa frequência são usados devido à maior penetração de objeto. Uma aplicação deste sistemas é, por exemplo, animais de pasto, podendo assim ler informação das etiquetas presentes nos animais a partir de leitores colocados no exterior, com uma frequência menor que 135 kHz.

Os sistemas de micro-ondas possuem um alcance de comunicação maior que os sistemas indutivos, variando entre os 2 a 15 metros. Contudo, e ao contrário dos sistemas indutivos, os sistemas de micro-ondas necessitam de uma bateria de reserva adicional porque, nestes sistemas, os leitores de RFID têm uma potência de transmissão que não é suficientemente para o funcionamento do *transponder*.

Os sistemas de RF têm a desvantagem de não poderem ser utilizados em locais onde existem outros campos de interferência eletromagnética, como os campos gerados por robôs de soldadura ou por fortes motores elétricos. Neste caso, os sistemas de micro-ondas apresentam-se como a melhor das soluções.

Na tabela 2.2 é possível observar-se informação mais detalhada acerca das quatro frequências de operação dos sistemas RFID.

Tabela 2.2: Características das frequências de operação dos sistemas RFID [21]

	Baixa Frequência < 135 kHz	**Alta Frequência - 13.65 MHz**	**Frequência Ultra Alta - 836 até 915 MHz**	**Micro-ondas 2.45 - 5.8 GHz**
Capacidade de Armazenamento	Desde 64 Bits para apenas leitura até 2 kBits para leitura e escrita.	Normalmente, leitura e escrita de tags com 512 Bits de memória.	Normalmente, leitura e escrita de tags com 32 Bits de memória.	A partir de 128 Bits para 32 kBits particionado.
Produtos Disponíveis	Apenas leitura ou leitura e escrita.	Apenas leitura ou leitura e escrita.	Apenas leitura ou leitura e escrita.	Apenas leitura ou leitura e escrita.
Transferência de Dados	Baixa taxa de transferência: menos de 1kBit/s (200 Bits/s)	Geralmente cerca de 25 kBits/s, contudo também existe a 100 kBits/s.	Cerca d 28 kBits/s.	Geralmente < 100 kBits/s, mas pode chegar até 1 MBits/s
Distância de leitura	Tipicamente meio metro. Para tags com baterias auxiliares até 2 metros.	Para tags com baterias auxiliares até um metro.	Para tags com baterias auxiliares até um metro.	Até cerca de 100 metros.
Modos de Leitura	Leitura de uma ou várias tag.	Leitura de uma ou várias tag.	Leitura de uma ou várias tag de modo omnidirecional.	Leitura de uma ou várias tag.
Limites Operacionais	-40º até +85º Celsius. Insensíveis a perturbações eletromagnéticas.	-25º até +70º Celsius. Pouco sensíveis a perturbações eletromagnéticas.	-25º até +70º Celsius. Sensíveis a perturbações eletromagnéticas ou outros sistemas que operem em frequências ultra altas.	-25º até +70º Celsius. Muito sensíveis a perturbações eletromagnéticas, sendo as ondas refletidas pelo metal e absorvidas pela água.
Aplicações	Processos de Manufatura. Identificação de veículos e contentores. Controlo de acessos. Identificação animal.	Monitorização. Parque Automóvel. Bagagens. Sector Logístico.	Sector Logístico. Monitorização de parque automóvel.	Controlo de acessos. Logística Militar. Portagens Automáticas.

2.3.5.2 Tipos da etiquetas

As etiquetas RFID, tal como mencionado anteriormente, podem ter alcances muito variados e podem considerar-se quatro tipos diferentes de acordo com o fornecimento de energia do *transponder*: passivas, ativas, semi-passivas e semi-ativas.

As etiquetas passivas não possuem qualquer tipo de alimentação, sendo alimentadas pelo sinal de RF que proveniente do leitor RFID e são as que têm maior durabilidade. Este tipo de etiquetas podem transmitir dados para o leitor através dois modos distintos de comunicação: *full-duplex/ half-duplex* ou SEQ. Em ambos os casos, a energia emitida pelo leitor RFID é utilizada para a transmissão de dados, sendo que quando o *transponder* não está no alcance da faixa do leitor, não é capaz de comunicar com o leitor RFID.

As etiquetas ativas possuem alimentação própria o que permite aumentar a distância de comunicação, contudo têm um tempo de vida limitado pelo duração da bateria (3 anos). Estes tipo de etiquetas utiliza a energia proveniente da bateria apenas para alimentar o chip e nunca para a transmissão de dados com o leitor. Com este tipo de etiquetas consegue-se operar com campos eletromagnéticos mais fracos do que com etiquetas passivas porque este deixa de ser utilizada para fornecer energia ao chip, e é apenas utilizado na transmissão de dados.

As etiquetas semi-ativas, funcionam como etiquetas ativas, mas vêm por defeito sem atividade, isto é, a alimentação que possuem encontra-se desligada. Assim, é necessário que se ativem as etiquetas deste tipo, passando depois a funcionar como uma etiqueta ativa, sendo que deste modo se consegue o prolongamento de funcionamento da bateria (até 5 anos).

As etiquetas semi-passivas possuem um fonte interna de alimentação que serve para alimentar circuitos mais complexos após a ativação da etiqueta e permite maiores distâncias de comunicação pois a energia recebida é utilizada apenas para a comunicação com o leitor.

Em suma, todos os tipos de *transponders* RFID precisam do campo magnético, eletromagnético, ou de micro-ondas do leitor para a transmissão de dados, sendo que as limitações físicas existentes são quem restringe substancialmente os intervalos de leitura.

2.3.6 Tipos de memórias de etiquetas

Do vasto leque de etiquetas RFID que existem no mercado, podem-se encontrar diversas capacidades de memória em diferentes etiquetas RFID, o que influencia, naturalmente, o preço das mesmas sendo que quanto maior memória a etiqueta tiver mais cara será.

As etiquetas RFID, podem ser dotadas de capacidade de memória entre poucos bytes e vários quilobytes. Contudo, e não menos importantes, também existem etiquetas RFID com 1 bit. Estas têm exatamente a capacidade de memória de um bit, sendo este suficiente para sinalizar a presença de uma etiqueta RFID no campo de um leitor RFID. As etiquetas RFID de 1 bit são frequentemente utilizadas para funções de monitoramento ou de sinalização, por exemplo, em lojas de roupa. Deste modo, este tipo de etiquetas possibilita a existência de vigilância eletrónica em lojas e empresas. Naturalmente, quando compramos um produto dotado de uma etiqueta deste tipo, a

etiqueta é desativada ou o bit é removido, de modo ao leitor RFID não detetar indevidamente etiquetas RFID de produtos pagos.

As etiquetas RFID com capacidade de memória podem ser graváveis ou não graváveis. As etiquetas RFID não regraváveis possuem a informação a armazenar, geralmente um identificador, desde que o chip é fabricado, não podendo ser alterado posteriormente. Por outro lado, as etiquetas RFID graváveis podem ser de três tipos: EEPROM's, SRAM ou Frams.

As etiquetas RFID podem ter acopladas indutivamente memórias programáveis apenas de leitura: EEPROMs. Este tipo de etiqueta graváveis, que dominam o mercado, têm duas desvantagens: requerem um elevado consumo de energia para a operação de escrita e têm um número limitado de ciclos de escrita, que variam entre o 100 mil e 1 milhão. O limite é imposto devido à deterioração interna do chip causada aquando do processo de apagamento dos dados pois para isto necessita de uma tensão elétrica mais elevada. Sempre que se grava um novo dado, o anterior é perdido. Este tipo de memória é capaz de armazenar entre 16 bytes e 8 Kbytes.

Um outro tipo de memórias usadas em etiquetas RFID são que utilizam Frams - memórias de acesso aleatório ferromagnético. Contudo estas foram utilizadas apenas em casos isolados. Embora necessitem de menos energia que as EEPROMs por um fator de 100 e tenham um tempo de escrita 1000 vezes mais baixo, este tipo de memória tem problemas ao nível da fabricação, o que tem impedido a sua introdução em massa no mercado.

O terceiro tipo de memórias utilizadas em etiquetas RFID são memória estáticas de acesso aleatório: SRAM. Usadas principalmente em etiquetas que operam através do sistema de micro-ondas, este tipo de memórias precisam de uma bateria auxiliar para a retenção dos dados a gravar. A grande vantagem deste tipo de memórias é que permitem ciclos de escrita muito rápidos, sendo que a capacidade de armazenamento varia entre os 256 Bytes e os 64 kBytes.

2.3.7 *Standards*

Na escala global do mercado atual, uma tecnologia para ser bem sucedida deve ser regida normas, standards, bem definidas, permitindo assim a sua proliferação em todos os mercados de uma forma mais ordenada, tornando a operação da tecnologia mais eficiente e segura. Assim, e de acordo com a *International Organization for Standardization* [25], as normas internacionais dão especificações de classe mundial para produtos, serviços e sistemas, de modo a garantir a qualidade, a segurança e a eficiência. Ou seja, um dos objetivos da normalização é facilitar o comércio internacional.

Na realidade do mercado dos RFID's, os maiores fabricantes oferecem sistemas proprietários, o que se traduz numa vasta gama de protocolos que regem os sistemas RFID. No reverso da medalha, existe a luta pela normalização dos protocolos por parte de organizações onde se destacam a ISO - *International for Standardization* e a EPC Global.

Na tabela 2.3 presente, podem-se observar as normas mais importantes lançadas pela ISO no âmbito da tecnologia RFID.

Tabela 2.3: Normas ISO aplicáveis aos sistemas RFID

[26] [27] [28]

Norma ISO	**Descrição**	**Data publicação ou última revisão da Norma**
ISO 11784	RFID para animais - estrutura de código	1996 [29]
ISO 11785	RFID para animais - conceção técnica	1996 [30]
ISO/IEC 14443-1	Cartões de identificação sem contacto - cartões com circuitos integrados - cartões de proximidade - características físicas	2013 [31]
ISO/IEC 14443-2	Cartões de identificação sem contacto - cartões com circuitos integrados - cartões de proximidade - potência do campo eletromagnético e interface do sinal	2011 [32]
ISO/IEC 14443-3	Cartões de identificação sem contacto - cartões com circuitos integrados - cartões de proximidade - inicialização e anti-colisão	2011 [33]
ISO/IEC 15693-1	Cartões de identificação sem contacto com circuitos integrados - cartões de vizinhança - características físicas	2010 [34]
ISO/IEC 15693-2	Cartões de identificação sem contacto com circuitos integrados - cartões de vizinhança - interface de ar e de inicialização	2013 [35]
ISO/IEC 15693-3	Cartões de identificação sem contacto com circuitos integrados - cartões de vizinhança - anti-colisão e protocolo de transmissão	2014 [36]
ISO/IEC 18001	Tecnologia da Informação – organização de itens de RFID – Perfil de Requisitos de Aplicação	2004 [37]
ISO/IEC 18000-1	Parâmetros gerais para comunicação por interface por ar	2008 [38]
ISO/IEC 18000-2	Parâmetros gerais para comunicação por interface por ar abaixo de 135 kHz	2009 [39]
ISO/IEC 18000-3	Parâmetros gerais para comunicação por interface por ar a 13,56 MHz	2010 [40]
ISO/IEC 18000-4	Parâmetros gerais para comunicação por interface por ar a 2,45 GHz	2015 [41]
ISO/IEC 18000-6	Parâmetros gerais para comunicação por interface por ar de 860 a 930 MHz	2013 [42]
ISO/IEC 15961-1	Gestão de itens de RFID - Protocolo de dados: protocolo de dados	2013 [43]
ISO/IEC 15962	Gestão de itens de RFID - Protocolo de regras de codificação de dados e funções de memória lógica	2013 [44]

Após uma análise à tabela 2.3, pode-se concluir que foram definidas normas para a identificação de pessoas (através dos cartões de identificação), animais ou gestão de itens com a tecnologia RFID.

As normas para os cartões de proximidade versam sobre as suas características físicas, a potência do campo eletromagnético e a interface do sinal, a inicialização e anti-colisão em caso de leituras simultâneas.

As normas para os cartões de vizinhança definem as suas características físicas, caracterizam a interface de ar e a inicialização, bem como os casos de anti-colisão e o protocolo de transmissão.

No caso da identificação de animais as normas versam sobre a estrutura do código e a conceção técnica da tecnologia RFID. Foram ainda estabelecidas normas para a gestão de itens nomeadamente acerca do protocolo de dados, regras de codificação de dados e funções lógicas de memória.

Por fim, foram também definidas normas gerais (arquitetura e definição de parâmetros) para a comunicação através do ar que utilizam frequências globalmente aceites e normas individuais de funcionamento gerais para diversas frequências de operação dos sistemas RFID: 135 kHz, 13.56 kHz, 2.45 Ghz e 860 a 930 MHz.

De notar que as normas são atualizadas ao longo do tempo e, como tal, devem ser consultadas na página oficial da ISO.

2.4 NFC - Near field communication

NFC é uma tecnologia que permite a troca de informações entre dispositivos sem a necessidade de uma ligação física entre os mesmos, bastando uma aproximação entre os dispositivos para haver uma conexão. A tecnologia supra-referida teve como base os sistemas RFID.

A tecnologia NFC utiliza, na comunicação entre dois sistemas/dispositivos, campos magnéticos alternados de alta frequência, isto é a 13.56 MHz. Numa conexão deste tipo a comunicação é feita até 10 cm, justificando-se assim o nome da tecnologia: *near field communication*. O objetivo da limitação na gama de alcance desta tecnologia foi para a tornar mais segura. [45]

Na figura 2.17 pode-se analisar o esquema físico de uma conexão NFC. As interfaces NFC, que operam a 13.56 MHz, quer para transmitir, quer para receber dados, possuem uma antena, antena essa que não é mais que um anel condutor.

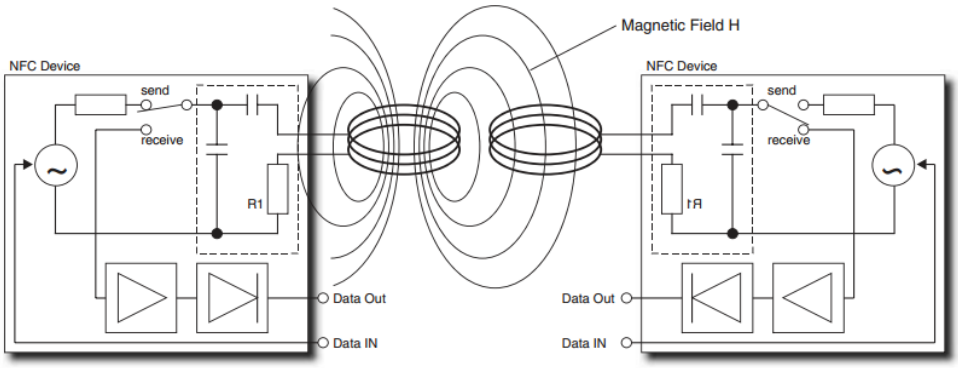


Figura 2.17: Esquema físico de uma conexão NFC [7]

A transmissão de dados entre dispositivos NFC pode ser feita de dois modos distintos: o modo ativo e o modo passivo. [46]

2.4.1 Modo Ativo

No modo ativo ambos os dispositivos geram um sinal de rádio próprio para a transmissão de dados. Numa primeira fase, um dos aparelhos inicia uma transmissão e é denominado iniciador. Uma corrente de alta frequência percorrerá a antena do iniciador, criando um campo magnético em torno desta antena. A antena do recetor, que está na gama de leitura do iniciador, irá ser percorrida por parte do campo magnético criado pelo iniciador. Assim, uma tensão U será induzida no circuito da antena do recetor e, no caso desta receber os sinais e comandos correspondentes ao de um iniciador NFC, o dispositivo estabelece uma conexão.

Numa conexão NFC, a amplitude do campo magnético é modulada, através da modulação ASK. Este processo é semelhante ao que ocorre entre um *transponder* e uma antena RFID, sendo que a grande diferença é que no caso do NFC o campo magnético alternado não garante a energia para a alimentação do micro-chip do recetor pois este tem uma fonte de alimentação própria.

Neste modo de operação a direção da transmissão é revertida para o recetor enviar dados para o iniciador NFC. Assim, o recetor tem de ativar o seu transmissor e o iniciador ativa a sua antena no modo de receção. Posto isto, ambas as interfaces criam, alternadamente, um campo magnético próprio sempre que enviam dados.

Na figura 2.18 pode-se observar um esquema ilustrativo da atuação de duas interfaces NFC em modo ativo.

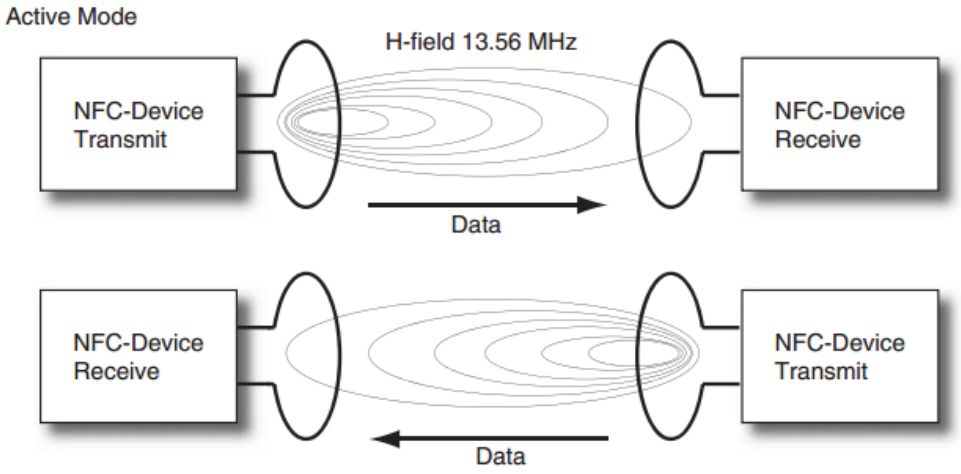


Figura 2.18: Esquema de conexão NFC em modo ativo [7]

2.4.2 Modo Passivo

No modo passivo o iniciador NFC também induz um campo magnético alternado para a criação da transmissão da dados. Neste modo também se utiliza a modelação ASK. A grande diferença é que, após a transmissão dos dados, o campo criado não é interrompido, continuando a ser gerado um campo magnético, mas não modulado. Desta feita, o recetor NFC pode transmitir dados para o iniciador através da geração da modelação do campo magnético, tal como se utiliza em alguns sistemas RFID.

Uma das grandes vantagens deste modo de operação é o facto de se puder negociar e alterar a qualquer momento qual das partes é que gera o campo magnético alternado o que se traduz numa enorme vantagem pois pode-se assim poupar bateria no caso de um dos dispositivos estar com a bateria fraca.

A tecnologia NFC é capaz de estabelecer conexões, não só com outros dispositivos NFC, mas também com *transponders* passivos que sigam a norma ISO/IEC 14443, ou seja, as etiquetas RFID. No caso de um dispositivo NFC estar no alcance do campo eletromagnético de um leitor RFID compatível com a norma ISO/IEC 14443, este também pode estabelecer uma conexão com o leitor RFID. Nesta situação específica, a interface NFC comportar-se-á como um recetor e transmitirá os dados para o leitor RFID através de uma modulação do campo magnético criado pelo leitor RFID. Assim é possível que leitores RFID comuniquem e troquem dados com interfaces NFC, sendo que do ponto de vista do leitor RFID, a interface NFC comporta-se como um cartão inteligente sem contacto. Por esta razão, este tipo de conexão chama-se modo de cartão. [7]

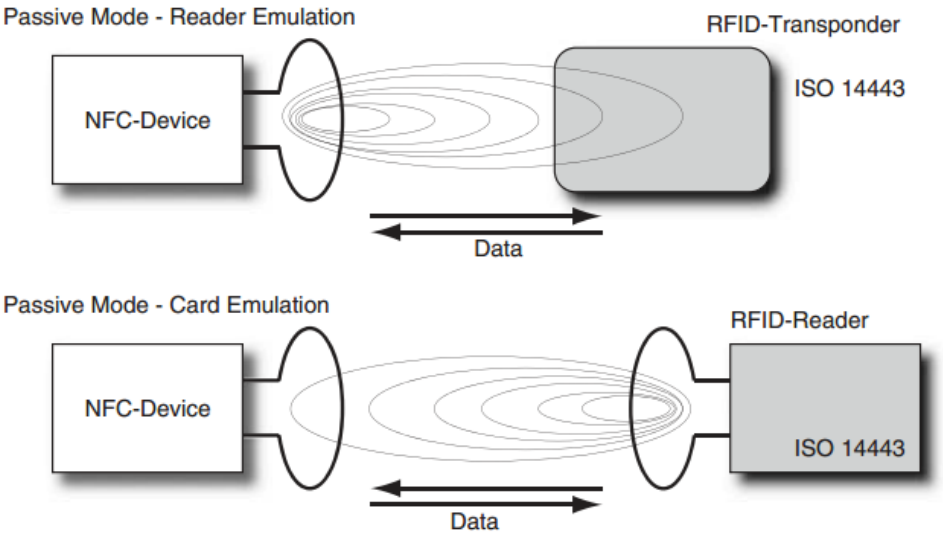


Figura 2.19: Esquema de conexões NFC em modo passivo [7]

Na figura 2.19 pode-se observar dois esquemas ilustrativos da atuação de interfaces NFC em modo passivo.

Capítulo 3

Arquitetura Proposta

Neste capítulo é apresentada uma análise de requisitos do sistema a ser desenvolvido que devem ser cumpridos. Posteriormente, é descrita uma proposta para a arquitetura geral das bancadas, bem como uma arquitetura individual para cada bancada de laboratório. Por fim, é também apresentada uma proposta da base de dados de suporte ao sistema e as principais funcionalidades da interface web a ser desenvolvida.

3.1 Análise de Requisitos

Nesta dissertação pretende-se o desenvolvimento de um sistema de identificação de objetos e pessoas para bancadas laboratoriais. Assim, e de modo a serem garantidas todas as especificidades pretendidas para o sistema, foi efetuado um levantamento dos requisitos que este deverá cumprir.

O sistema a ser desenvolvido deverá ser autónomo, não necessitando de outros sistemas para o seu funcionamento. Além disto, será também um sistema modular e escalável, permitindo que se adapte facilmente a qualquer laboratório, independentemente do número de bancadas que o compõe. Assim, deve ser possível a qualquer momento que se acrescentem novas bancadas ao sistema de gestão do laboratório, encarando cada nova bancada como um novo módulo do sistema, com fácil e rápida configuração.

O funcionamento geral do sistema não deverá depender do tipo de leitores de identificação de NFC e RFID utilizados, ou seja, deve-se permitir que estes sejam trocados, por exemplo, por outros de outras marcas ou com maior alcance de leitura. Para esta troca ser possível, poderá ser acrescentado *software*, com o único objetivo de fazer funcionar o novo leitor, sem alterar o modo de funcionamento do *software* previamente implementado. Assim, a troca dos leitores deverá ser semelhante a um sistema do tipo *plug and play*, isto é, "ligar e usar".

Devido à existência de diversos tipos de bancadas laboratoriais, poderá existir a necessidade de mais do que um leitor para cada tipo de tecnologia de identificação, especialmente o leitor da tecnologia RFID para a identificação de objetos. Esta necessidade pode surgir em casos de bancadas com grandes dimensões, sendo vantajoso que existam várias zonas de leitura. Deste

modo, facilitar-se-á a identificação dos objetos utilizados pois, o utilizador da bancada poderá utilizar mais do que um local na bancada para a identificação dos objetos que utilizou.

Para cada bancada laboratorial, e dependendo das suas características, o sistema deverá ser capaz de gerir eficientemente o acesso à bancada. Assim, por exemplo, para bancadas que tenham gavetas com fechaduras eletrónicas, o sistema será capaz de abrir automaticamente a fechadura das gavetas só quando um utilizador estiver a utilizar a bancada. Este tipo de controlo poderá também ser aplicado em outros casos como: abertura automática da janela de uma hotte química ou ligação do sistema de extração de fumos da bancada (nos casos em que exista).

Todas as bancadas de laboratório estarão ligadas entre si a uma rede local TCP/IP. Deste modo, poder-se-á utilizar esta rede para a comunicação entre as bancadas e o registo, ou consulta, dos dados armazenados na base de dados. A ligação das bancadas à rede TCP/IP poderá ser efetuada através de ligação físicas à rede, recorrendo a portas *ethernet*, ou então, através de um ligação via wifi à rede TCP/IP.

3.1.1 Base de Dados

O sistema a ser desenvolvido deverá permitir uma gestão eficiente dos acessos às bancadas de laboratório, sendo capaz de registar reservas, identificar as pessoas que utilizam as bancadas, bem como os objetos utilizados durante a realização de um dado trabalho.

Assim, o sistema a ser desenvolvido, além dos leitores para a identificação de pessoas e objetos, deverá também armazenar informação, sendo que esta deverá guardar os seguintes dados:

- Bancadas Laboratoriais
    1. lista de todas as bancadas de laboratório existentes;
    2. estado de cada bancada (operacional ou inoperacional);
    3. registo das reservas feitas por utilizadores do laboratório para utilização futura de uma bancada;
    4. registo de utilizações das bancadas, isto é, guardar a hora em que uma bancada foi utilizada por um utilizador. Neste caso, deve também ser guardado na base de dados, o identificador RFID de todos os objetos utilizados durante a realização de um determinando trabalho, de modo a saber-se quais os objetos utilizados.
- Pessoas
    1. dados pessoais dos utilizadores das bancadas, como por exemplo o nome, a morada, o número de telemóvel, o email, um *username* e uma *password*;
    2. identificador NFC de cada pessoa;
    3. tipo de utilizador do laboratório. As pessoas que utilizam as bancadas de laboratório, também designadas utilizadores, deverão ser consideradas de acordo com as permissões que possuem. Deverão então ser criados dois níveis de permissões que definirão o grau de usabilidade da interface a desenvolver, podendo os utilizadores ser designados como colaboradores ou como administradores do sistema.
- Objetos

1. inventário com os objetos existentes no laboratório e que se pretendem identificar sempre que sejam utilizados em trabalhos desenvolvidos numa bancada. Os objetos a ser identificados são maioritariamente frascos não metálicos com reagentes do tipo sólido ou líquido;
2. identificador RFID de cada objeto.

3.1.2 Interface Web

Será implementada uma interface web que permita visualizar os dados armazenados pela base de dados e efetuar ações como:

- reserva de bancadas;
- cancelamento de reservas;
- adicionar novos utilizadores de bancadas;
- adicionar novas bancadas de laboratório;
- adicionar novos objetos.

A interface web a ser desenvolvida deverá ser intuitiva, de modo a que todos os utilizadores possam utiliza-lá de forma rápida e eficaz. As funcionalidades disponíveis na interface web serão diferentes conforma o tipo de permissões que cada utilizador tem. Não obstante, cada utilizador deverá conseguir visualizar o seu histórico, desde as utilizações já efetuadas, até às reservas que têm registadas.

3.1.3 Utilizadores do laboratório

Tal como já referido, deverão existir dois tipos de utilizadores do laboratório de acordo com as suas permissões. São definidos como colaboradores os utilizadores das bancadas de laboratório que não têm permissões de administrador do sistema, bem como, as pessoas responsáveis pela sua limpeza. Os colaboradores poderão utilizar a interface do sistema para efetuar ações elementares como reservar ou cancelar uma reserva de uma bancada de laboratório, consultar o seu histórico de utilizações de bancadas ou visualizar as reservas futuras que se encontram registadas na base de dados.

Os administradores poderão efetuar o conjunto de ações que os colaboradores no que respeita à interface do sistema, tendo também permissões ao nível de gestão do laboratório, como:

- cancelar reservas de bancadas aos colaboradores;
- introduzir um novo colaborador, um novo objeto ou um novo equipamento no sistema de gestão do laboratório;
- retirar uma, ou várias, bancadas de laboratório de funcionamento;
- definir as bancadas a que cada colaborador terá acesso;
- nomear um colaborador como administrador do sistema;
- retirar as permissões de administrador do sistema a um administrador, tornando-a assim um colaborador;

- efetuar reservas nas bancadas de laboratório para que se efetuem operações de manutenção/ reparação das bancadas.

3.1.4 Identificação de Pessoas

A identificação de pessoas em cada bancada de laboratório será feita recorrendo à tecnologia NFC, através de *smartphones* ou de cartões NFC. A escolha da **tecnologia NFC** deveu-se ao facto desta ser nova, estar em crescimento e cada vez mais presente no mercados dos *smartphones*.

Para a identificação das pessoas será utilizado o identificador NFC presente em cada *smartphone* ou cartão NFC. De acordo com a norma ISO/IEC 14443 - A, cada etiqueta NFC é composta por três partes distintas:

1. ATQA - identificador do fabricante;
2. SAK - identifica o tipo de etiqueta, com por exemplo: MIFARE Mini ou MIFARE classic 1k;
3. *Unique Identifier*: UID - é o identificador de cada tag NFC com tamanho de 4 bytes, sendo comum a sua representação em hexadecimal. [47]

Ao serem utilizados os *smartphones* para o reconhecimento de pessoas, está-se a "aproximar" o sistema instalado nas bancadas ao utilizador, ao mesmo tempo que lhes evita algum possível transtorno, como o esquecimento de um cartão de identificação. No entanto, nem todos os laboratórios permitem o uso de *smartphones* no seu interior, sendo que, nesses casos, o acesso poderá ser feito através de cartões NFC, implicando assim um investimento suplementar em cartões NFC. Contudo, e tendo em conta o investimento feito no sistema, a aquisições de cartões NFC para os colaboradores não o tornará muito mais caro, visto que cada cartão NFC custa cerca de 0.50/0.60€. [48]

A identificação de um utilizador numa bancada só deverá ser considerada válida se este tiver efetuado previamente uma reserva da bancada para aquela hora. Ou seja, caso o utilizador não tenha efetuado uma reserva, o sistema de identificação de pessoas não validará a tentativa de utilização da bancada porque não existe uma reserva. Neste caso, o leitor NFC deverá continuar a efetuar leituras de identificadores NFC, até existir algum identificador NFC que esteja associado a uma reversa registada na base de dados para utilização da bancada.

3.1.5 Identificação de Objetos

Os objetos a serem identificados durante a utilização de uma bancada de laboratório serão essencialmente frascos não metálicos, comummente de plástico ou, em casos menos comuns, de vidro, que armazenam consumíveis reagentes do tipo líquido ou sólido e desprovidos de movimento próprio. Cada objeto terá colada uma etiqueta RFID de reduzidas dimensões, sendo que esta tem um UID associado que é único e com 16 dígitos em hexadecimal, que será utilizado para a identificação do objeto através do(s) leitor(es) RFID presente(s) na bancada. O sistema deverá ser capaz de identificar mais do que um objeto em simultâneo, ou seja, deverá ser dotado se um sistema anti-colisões na leituras de etiquetas RFID permitindo assim registar na base de dados

todos os objetos utilizados, mesmo que estes estejam na zona de alcance de leitura do leitor ao mesmo tempo.

3.2 Arquitetura geral - Bancadas de laboratório

Após uma análise aos requisitos gerais propostos em 3.1, foi definida uma arquitetura para o desenvolvimento do sistema de identificação de objetos e pessoas. De modo a este ser modular e escalável, optou-se por considerar-se cada bancada de laboratório como uma parte do sistema, dotando-a com uma plataforma computacional capaz de adquirir e processar os dados provenientes dos leitores instalados nessa bancada para a identificação de pessoas e objetos.

Focando no conjunto das bancadas de laboratório que estarão ligadas a uma rede local, optou-se pela criação de uma base de dados numa plataforma computacional que já fosse utilizada previamente numa das bancadas, permitindo assim uma otimização dos recursos. Esta plataforma computacional, doravante *bancada laboratorial - servidor*, terá também armazenada a interface para a gestão de reservas das bancadas.

A interface a ser implementada é uma página web, pois é uma forma eficaz e muito utilizada atualmente como meio de apresentar informação a um utilizador. O acesso à página web será feito através de um *username* e uma *password* que cada utilizador possuirá, sendo os dados de acessos disponibilizados pelos administradores do sistema. Deste modo, só será necessário que uma plataforma computacional esteja sempre ligada, a da *bancada laboratorial - servidor*, para a página web e a base de dados se encontrarem acessíveis, permitindo que todas as outras plataformas estejam desligadas sempre que o laboratório não se encontrar em funcionamento.

Durante a conceção da arquitetura geral do sistema ilustrado na figura 3.1, e de modo a ser possível que todas as bancadas de laboratório consigam aceder à base de dados, existiu a necessidade de se definir um endereço IP estático para a *bancada laboratorial - servidor*, permitindo assim que todas as plataformas computacionais das outras bancadas consigam aceder à base de dados do sistema. Por outro lado, as outras bancadas laboratoriais terão um endereço IP atribuído dinamicamente pelo servidor DCHP da rede TCP/IP já existente. Estas bancadas serão designadas como *bancadas de laboratório - clientes*.

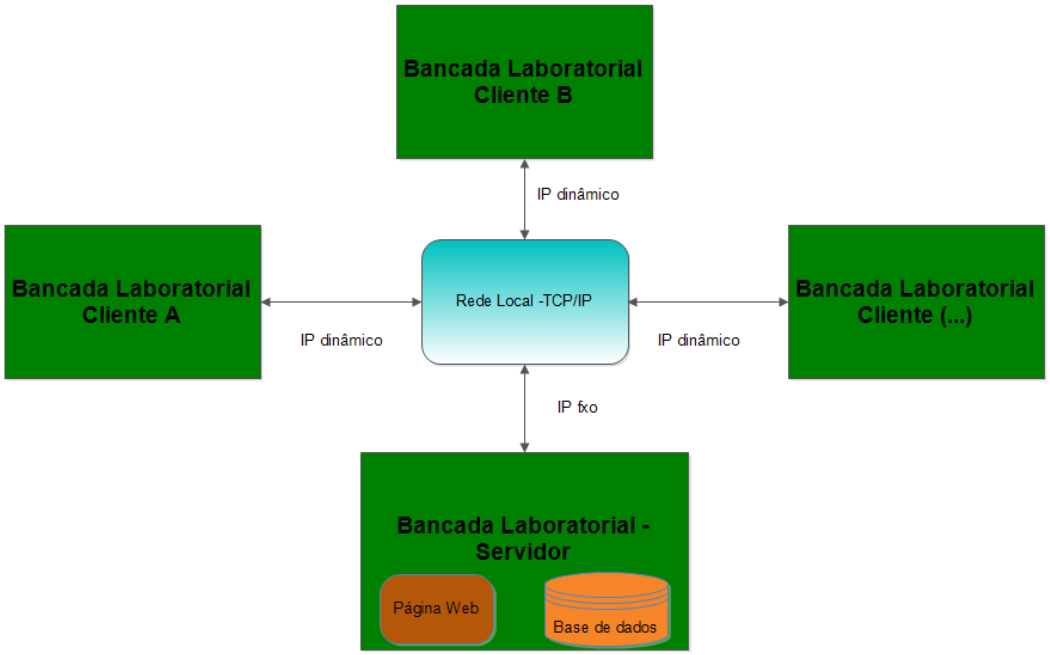


Figura 3.1: Imagem ilustrativa da arquitetura geral do sistema

3.3 Arquitetura - bancada laboratorial

De acordo com os requisitos do sistema, este deve ser independente do tipo de leitor NFC ou RFID utilizado em cada bancada laboratorial. De modo a cumprir esta especificação, foi pensado implementar-se em cada bancada um sistema com uma arquitetura do tipo *cliente-servidor*.

A escolha de uma arquitetura do tipo cliente-servidor para cada bancada laboratorial, justifica-se devido às vantagens que apresenta face a outros tipos de arquiteturas. Os clientes, cada um com software específico, serão responsáveis tanto pela gestão dos atuadores, como pela recolha de dados provenientes dos sensores e dos leitores NFC e RFID. O servidor será responsável pela processamento de toda a informação proveniente dos clientes, sendo que as vantagens mais significativas deste tipo de arquitetura são:

- a criação de um sistema expansível, através do desenvolvimento de novos clientes;
- possibilidade de retirar/substituir clientes de funcionamento, através da eliminação/substituição do cliente em questão;
- maior fiabilidade do sistema: só o servidor acederá à base de dados, não havendo assim acessos simultâneos provenientes da mesma bancada, evitando excessos de pedidos de ligação à base de dados;

Não obstante, o modelo escolhido apresenta também desvantagens, sendo a mais crítica, que se o servidor for desligado, o sistema deixa de funcionar. Outro tipo de problemas associados a este modelo é em casos de sobrecarga de pedidos enviados ao servidor por parte de clientes.

Na figura 3.2, pode-se observar o esquema do modelo *cliente-servidor* a ser implementado. Nela, pode observar-se o *servidor* que terá ligado a si um conjunto diverso de *clientes*: leitores,

sensores ou atuadores. O número de *clientes* que se podem ligar ao *servidor* não é limitado pelo sistema, sendo apenas limitado pelo número de interfaces de ligação que a plataforma computacional suporta. O *servidor* ligar-se-à ainda à base de dados do sistema de modo a aceder à informação que esta armazena.

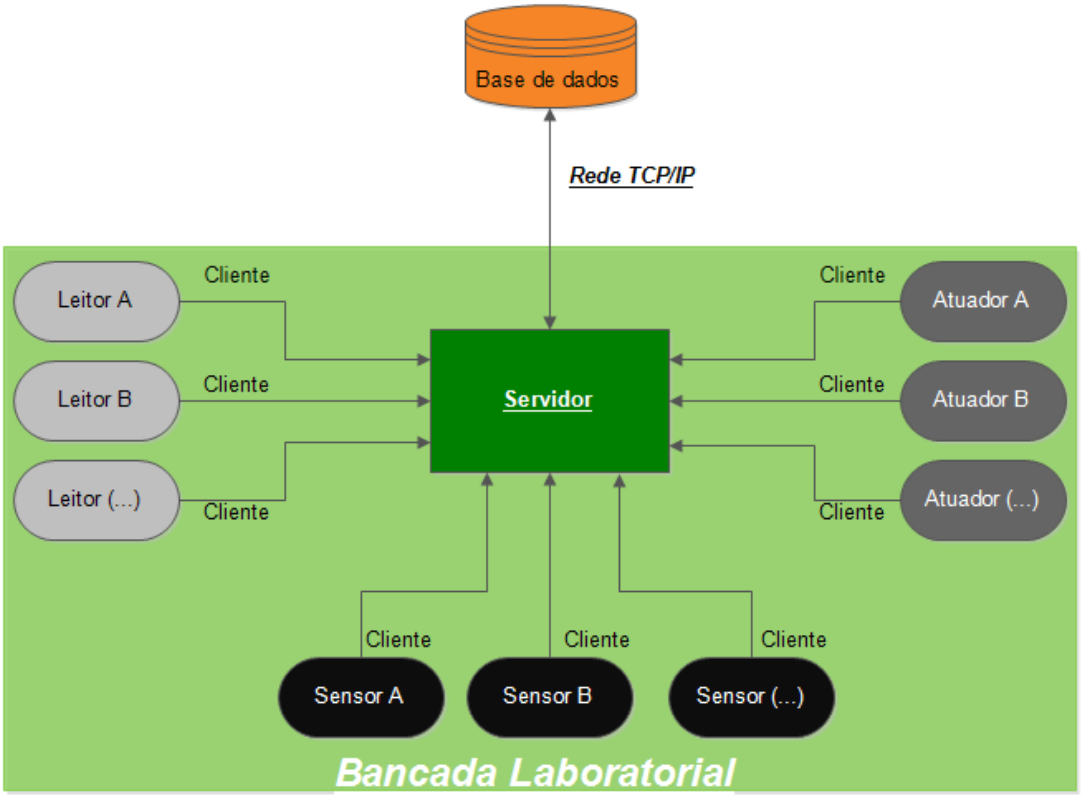


Figura 3.2: Imagem ilustrativa dos componentes de uma bancada laboratorial

Os leitores a serem incorporados no sistema serão leitores de NFC ou RFID, de modo a identificar pessoas ou objetos, respetivamente. Por outro lado, os sensores poderão ser botões, ou outro tipo de sistemas, que permitirão a um utilizador desligar a sua sessão numa bancada, ou então, desligar a plataforma computacional da bancada em que esteja inserida. Por fim, os clientes responsáveis pela gestão de atuadores, são aqueles que terão de gerir o estado dos componentes de cada bancada laboratorial, como por exemplo: a abertura e fecho automático da janela de uma *hotte química*, a ligação do sistema de extração de fumos da bancada ou a abertura e fecho automático das gavetas de uma bancada.

Cada *cliente* responsável pela gestão de um leitor ou de um sensor, terá como princípio de funcionamento a recolha de dados provenientes do leitor, ou sensor, enviando-os depois para o *servidor*. Durante o processo de envio, e tendo em consideração o protocolo a implementar, o *servidor* ao analisar a informação recebida será capaz de identificar se a trama recebida é proveniente de um leitor ou de um sensor, procedendo depois ao tratamento da informação que recebeu.

Os *clientes-atuadores* serão responsáveis pela gestão do acesso aos constituintes da bancada, como por exemplo gavetas com fechadura eletrónica ou abertura da janela frontal de uma hotte química. Este tipo de clientes funcionarão de forma um pouco diferente e serão simultaneamente clientes e servidor. Esta dualidade existe porque quando o sistema inicia, os *clientes* que gerem atuadores, enviaram uma trama ao *servidor* de modo a "informá-lo" que é um atuador, comportando-se até aqui como um cliente. Posteriormente, quando o *servidor* precisar de mudar o estado de um atuador do sistema, o *servidor* enviará uma trama ao cliente que gere o atuador em questão, com informação acerca da ação a ser tomada, sendo que o cliente interpretará a trama de acordo com o protocolo a implementar. Durante esta fase, que é mais demorada, os *clientes-atuadores* funcionaram como um servidor porque irão atuar sobre o estado de um dos constituintes da bancada.

Para a implementação do modelo *cliente-servidor*, será desenvolvido um protocolo que garanta a comunicação eficaz entre o *servidor* e os seus *clientes*. Este protocolo, tal como se pode ver na figura 3.3, terá por base o envio de tramas com duas partes distintas de informação.

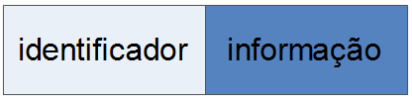


Figura 3.3: Ilustração da constituição do protocolo utilizado na comunicação entre clientes-servidor e servidor-clientes

Na tabela 3.1, pode-se encontrar uma descrição das partes constituintes da trama do protocolo. Para acrescentar, ou substituir, clientes leitores, sensores ou atuadores, terá de ser respeitado o protocolo pelo novo cliente desenvolvido.

Tabela 3.1: Descrição da trama do protocolo

Constituintes da trama	**Descrição**
Identificador	Os diferentes tipos de clientes leitores, sensores ou atuadores, bem como o servidor, terão um identificador único de modo a indicar a origem da trama. Este identificador terá o tamanho de 2 *bytes*.
Informação	Parte da trama, de tamanho variável, que contém a informação que se pretende enviar. Conhecendo-se a origem da trama, poder-se-á saber o tamanho do campo "informação", pois este é pré-definido e só depende se é proveniente de identificadores NFC, identificadores RFID, do servidor ou de sensores.

Na figura 3.4, pode-se visualizar um exemplo de uma trama do protocolo desenvolvido. Esta trama contém o identificador *10* e a informação de um UID RFID - *E00780ACDDE83275*.

Figura 3.4: Imagem ilustrativa de um trama do protocolo desenvolvido enviada por um cliente - leitor RFID

O modelo cliente-servidor deverá ainda permitir acrescentar, ou substituir, leitores, sensores ou atuadores em cada bancada laboratorial de forma simples e rápida. Deste modo, previnem-se, por exemplo, casos em que o *hardware* foi retirado do mercado possibilitando a sua substituição, evitando tornar o sistema obsoleto devido a este tipo de fatores. Para acrescentar, ou substituir um leitor, sensor ou atuador, será necessário o desenvolvimento de um novo cliente por forma a suportar o funcionamento do novo leitor, sensor ou atuador. Assim, e tal como referido em 3.1, a troca de leitores será semelhante ao mecanismo de *plug and play*, sendo necessário acrescentar um novo cliente ao servidor, sem necessidade de modificar o *software* implementado previamente.

Em casos de substituição de um leitor, sensor ou atuador, o cliente responsável por este, deverá ser eliminado pois já não será mais necessário ao funcionamento do sistema. Não obstante, será acrescentado um novo cliente para suportar o funcionamento do novo leitor, sensor ou atuador.

3.4 Base de dados

De acordo com os requisitos do projeto, foi implementada uma base de dados de modo a permitir o registo de todas as informações necessárias ao funcionamento do sistema. Tal como referido, todas as bancadas do laboratório estarão ligadas numa rede TCP/IP, pelo que todas as bancadas se poderão ligar à base de dados que suporta o sistema.

A base de dados deve conter uma entidade para o registo dos dados pessoais de todos os utilizadores do laboratório, criando assim um banco de dados dos utilizadores com os campos mais importantes como o nome, morada e contacto do utilizador. Ainda acerca dos utilizadores, a base de dados deverá permitir o armazenamento de informações relativas aos dados de acesso do utilizador à página web, *username* e *password*, bem como o identificador NFC de cada utilizador. Por fim, a base de dados estará preparada para armazenar a informação de que o utilizador tem, ou não, permissões de administrador do sistema.

Deverá ser também possível registar na base de dados informação acerca das bancadas que existem no laboratório, através de uma designação a ser escolhida pelo administrador do sistema. A base de dados deverá ainda permitir o registo dos dados relativos aos objetos que existam no laboratório, nomeadamente o nome e uma descrição do mesmo e o identificador RFID que cada objeto tem associado a si.

De modo a garantir a gestão de acessos às bancadas de laboratório, a base de dados deverá também permitir o registo das reservas que cada utilizador efetua, com a informação do dia, hora

de início e fim da reserva e a bancada pretendida. Para cada utilização de uma bancada de laboratório, a base de dados estará também preparada para armazenar a informação acerca da hora de início e de fim de utilização de uma bancada de laboratório, associado a esta informação o utilizador que está a utilizar a bancada, bem como a bancada em questão e os objetos que são colocados na(s) zona(s) de leitura do(s) leitor(es) RFID.

Por fim, a base de dados deverá ainda ter a capacidade de associar a cada utilizador as bancadas que este pode utilizar, sendo que sempre que um novo utilizador é introduzido na base de dados, este não tem acesso a nenhuma bancada, da mesma forma que uma bancada laboratorial quando é inserida não tem utilizadores que a possam utilizar. Assim, nestes casos, o administrador do sistema terá de fazer a gestão deste tipo a permissões.

Na figura 3.5 é possível observar-se o modelo relacional da base de dados implementada, onde o nome das entidades do modelo relacional estão com o fundo a azul e o nome das relações têm o fundo cor de rosa. Todas as entidades e relações têm de ter, pelo menos, uma chave-primária que é um atributo não nulo e unívoco da tabela.

De seguida, serão enumerados os atributos [1] que compõem cada entidade e relação da base de dados.

- **Entidades**
  - **Equipamento:** entidade constituída por 3 atributos, tendo como chave-primária um **id**[2] , guardando uma designação para cada bancada de laboratório no atributo **nome** e o estado da bancada no atributo **operacional** que guardará a informação "0" ou "1", conforme a bancada esteja inoperacional ou operacional, respetivamente.
  - **Colaborador:** guarda informações específicas de todos os colaboradores do laboratório, tendo como chave-primária um **id**. Cada colaborador terá na base de dados os atributos **nome**, **telemovel**, **email** e **morada**, para gestão dos dados de cada um; os atributos **nfc1**, **nfc3**, **nfc3**, **nfc4** para associar um identificador NFC ao colaborador, e ainda os atributos ***username*** e ***password***, para o colaborador se autenticar na página web. Por fim, ainda existe o campo **admin** que terá um de dois estados: 0 - se o utilizador não for administrador do sistema e 1 se o utilizador for administrador do sistema. Por defeito, os novos utilizadores não são administradores do sistema.
  - **Objeto:** entidade constituída por 4 atributos, tendo como chave-primária um **id** - identificador, guardando também na base de dados o nome, o identificador da etiqueta RFID e uma descrição de cada objeto existente na bancada, através dos atributos **nome**, **rfid** e **descrição**, respetivamente.
- **Relações**
  - **Reservas:** regista a reserva de uma bancada laboratorial efetuada por um colaborador. Para isso utiliza as chaves-primárias: **aux**[3], **id_equipamento** e **id_colaborador**.

[1] variáveis em que são guardadas as informações
[2] identificador
[3] auxiliar

Ainda tem os atributos **dia**, **hora_ini** [4] e **hora_fim**[5], de modo a registar o intervalo de tempo que o colaborador quer reservar uma dada bancada, num determinado **dia**. Podem também ser efetuadas reservas por parte do administrador do sistema, de modo a reservar uma bancada para a reparar ou então para impedir o acesso à mesma num certo horário.

- **Utilizacoes:** regista a utilização de uma bancada laboratorial efetuada por um colaborador, quando existe uma reserva prévia. Para isso, utiliza as chaves-primárias **id**, **id_equipamento** e **id_colaborador**. Também tem os atributos **dia**, **hora_ini** e **hora_fim**, de modo a registar o dia em que a bancada foi utilizada, bem como a hora de início da utilização e a hora de fim.
- **Utilizou:** tem como chaves-primárias os atributos **id_utilizacoes** e **objetos** para registar os identificadores RFID dos objetos utilizados por um colaborador, numa dada utilização.
- **Permissoes:** permitir ao administrador do sistema do laboratório restringir o acesso de certos colaboradores a certas bancadas de laboratório; tem os atributos **id_equipamento** e **id_colaborador**, que são também as chaves-primárias.

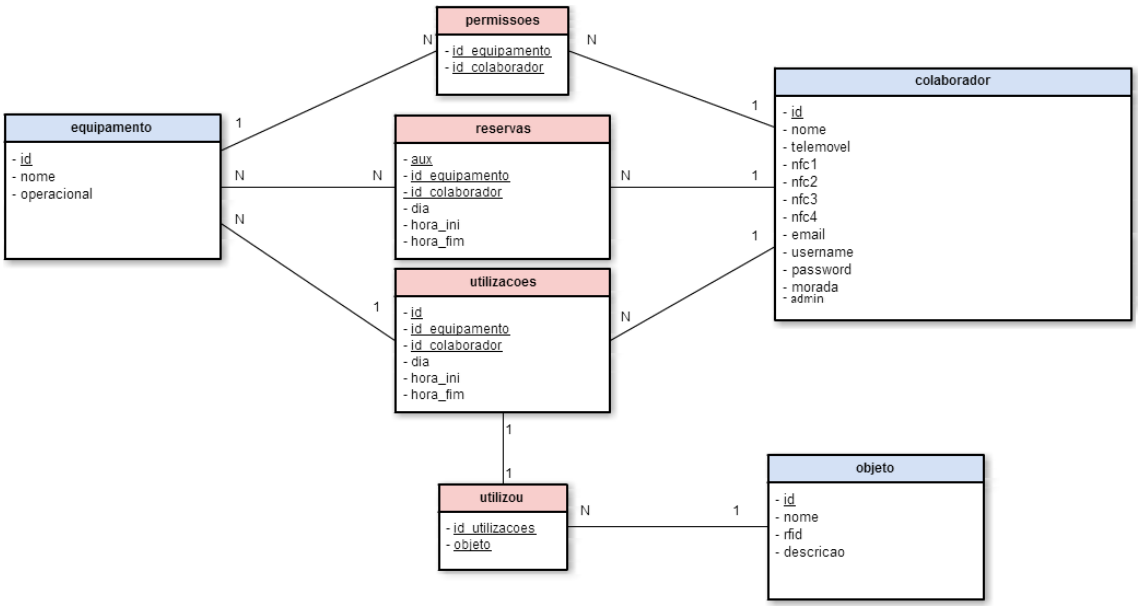


Figura 3.5: Modelo Relacional da Base de Dados

3.5 Interface Web

A interface web a ser desenvolvida tem como principal função a interação com os colaboradores e com o administrador do sistema, de acordo com os requisitos definidos em 3.1. Como já

[4] hora de início
[5] hora de fim

referido, escolheu-se desenvolver uma página web para interface do sistema, sendo que esta terá características diferentes conforme o tipo de utilizadores. Assim, as funcionalidades da página web de acordo com o tipo de utilizador serão:

- Administrador do sistema:
  - adicionar novos colaboradores;
  - associar identificador NFC a um colaborador;
  - registar novas bancadas de laboratório;
  - gerir o estado operacional das bancadas permitindo, por exemplo, efetuar um reparação ou mesmo retirar de funcionamento uma bancada por tempo indeterminado;
  - definir o horário de funcionamento para cada bancada;
  - registar novos objetos;
  - associar um identificador RFID a um objeto novo;
  - visualizar o histórico de reservas das bancadas;
  - efetuar reservas em bancadas laboratoriais;
  - consultar ou cancelar reservas que já têm efetuadas;
  - dar/retirar permissões de utilização nas bancadas laboratoriais;
  - nomear novos administradores;
  - remover administradores;
  - aceder ao histórico de utilizações das bancadas.
- Colaboradores:
  - efetuar reservas em bancadas que tenham permissão;
  - consultar ou cancelar as reservas que tenham sido efetuadas;
  - visualizar o seu histórico de utilização das bancadas do laboratório.

As reservas de bancadas por parte dos utilizadores na interface web deverão poder ser feitas para qualquer dia da semana num intervalo de horas correspondente ao horário de funcionamento do laboratório. A interface web não deverá permitir reservas sobrepostas nas bancadas, ou seja, quando um utilizar tentar fazer uma reserva para um dia, só poderá fazê-la nos intervalos de tempo em que a bancada está livre. Por fim, cada utilizador só poderá efetuar reservas nas bancadas laboratoriais em que tiver permissões para as utilizar.

3.6 Sumário

De acordo com o descrito ao longo do capítulo 3 desta dissertação, será implementado um sistema de gestão de bancadas laboratoriais composto por várias plataformas computacionais ligadas a uma rede TCP/IP, sendo cada uma delas será responsável pela gestão de acessos a uma bancada de laboratório. Cada plataforma terá conectados a si leitores, sensores e atuadores de modo a identificar objetos ou pessoas e gerir o estado da bancada, conforme esteja a ser utilizada ou não. As plataformas computacionais comunicarão com uma base de dados, para consultar as reservas efetuadas nas bancadas de laboratório. Por fim, existirá uma interface web para o agendamento da

utilização das bancadas, consulta do histórico de utilizações e outras funcionalidades relevantes para o sistema de gestão de acesso às bancadas de laboratório.

Capítulo 4

Implementação da Arquitetura

O trabalho desenvolvido para o cumprimento dos objetivos propostos nesta dissertação será explicado de seguida, através de três secções. Na primeira, será apresentada a plataforma computacional selecionada, bem como dos leitores NFC e RFID utilizados. Na segunda, será explicado o trabalho implementado na plataforma computacional a instalar em cada bancada, e na terceira, será descrita a abordagem relativa à interface web desenvolvida, bem como a da base de dados criada.

4.1 Seleção de *hardware*

Tal com explicado no capítulo 3, cada bancada de laboratório terá uma plataforma computacional. Assim foi necessário fazer-se uma análise de mercado com o intuito de se selecionar uma plataforma computacional capaz de satisfazer a análise de requisitos já enunciada. Será também explicada a escolha dos leitores NFC e RFID utilizados no âmbito desta dissertação.

4.1.1 Plataforma Computacional

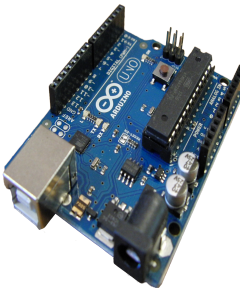
De modo a suportar o funcionamento do sistema em cada bancada de laboratório, foi escolhida uma plataforma computacional capaz de recolher, analisar e processar os dados provenientes dos leitores e detetores, bem como interagir com os atuadores. Assim, após uma análise da oferta existente no mercado, selecionaram-se três possíveis plataformas:

1. *Arduino Uno*: micro-controlador programável. A sua função base é a leitura de dados, sendo que para o processamento destes poderá ser utilizado, por exemplo, um computador ou um Raspberry Pi. [49]
2. *Raspberry Pi 2 B*: pode-se adicionar um teclado, rato e ecrã, ficando-se com um pc a custo bastante reduzido. É considerado como sendo um "mini-computador"devido às suas reduzidas dimensões, possuindo interfaces de comunicação como saída de áudio, HDMI (*High-Definition Multimedia Interface*), USB, RCA ou porta *ethernet*. É uma tecnologia recente no mercado, com potencial de crescimento. [50]

3. *Beagle Bone Black*: semelhante ao Raspberry Pi 2 B. Possui mais portas de *input/output*(I/O) e tem maior capacidade de processamento; contudo o seu custo é superior. [51]

Tabela 4.1: Características técnicas das plataformas computacionais

[49] [50] [51] [52] [53] [54]

	Arduino Uno	Raspberry Pi 2 B	Beagle Bone Black
Imagem ilustrativa			
Processador	ATmeg 328	ARM Cortex-A7 Quad-Core	AM335x ARM Cortex A8
Clock	16 MHz	900 MHz	1 GHz
RAM	2 KB	1 GB	512 MB
Flash	32 KB	Micro SD	2BG + Micro SD
Ethernet	Via shield	Sim	Sim
Portas I/O	14 digitais, 6 analógicas	40 digitais	65 digitais, 7 analógicas
USB	n/a [0]	4	1
Audio	n/a [0]	HDMI, Analog	HDMI
Video	n/a [0]	HDMI, RCA	Mini-HDMI
Dimensão	68.6x53.4 (mm)	85.6x56 (mm)	86.36x54.61 (mm)
Sistema Operativo	n/a[0]	Linux	Android, Linux, Windows, Cloud9
Custo	24.60€[55]	51.60€[56]	70.05€[57]

Após uma análise da tabela 4.1 e conhecendo as características das plataformas computacionais referidas, o Arduino revela-se a opção menos indicada, porque foi projetado para leitura de dados, ao contrário das outras plataformas que suportam a leitura e o processamento de dados. Contudo o Arduino poderia suportar uma aplicação como a que se pretende implementar, mas teria de ser utilizado em conjunto com uma outra plataforma, como por exemplo um computador, de modo a que o computador processa-se os dados recolhidos pelo Arduino o que tornaria o sistema mais complexo, do que no caso de só se utilizar uma única plataforma.

Assim, a escolha ficou restrita entre o Raspberry Pi 2 B e o Beagle Bone Black. De modo geral, o Beagle Bone Black é mais completo pois tem mais capacidade de processamento, mais memória ram, mais portas I/O. Contudo, o Raspberry Pi 2 B é mais barato e possui todas as características necessárias para dar suporte ao projeto. De realçar ainda, que ambos possuem uma

[0] não aplicável

porta que suporta ligações do tipo *Ethernet*, úteis para a ligação das bancadas de laboratório à rede TCP/IP [1]. A ligação à rede TCP/IP também poderia ser efetuada através de wifi, no entanto, para isso, seria necessário acrescentar um módulo wifi à plataforma computacional. Deste modo, a plataforma computacional escolhida foi o Raspberry Pi 2 B e, assim sendo, o sistema operativo utilizado no desenvolvimento desta dissertação foi o Linux.

4.1.2 Leitor NFC

A tecnologia NFC permitirá o reconhecimento de pessoas através do identificador NFC, associado por defeito, a um *smartphone* ou a um cartão NFC.

Após uma análise dos leitores existentes no laboratório da Faculdade de Engenheira da Universidade do Porto - FEUP, foram selecionados dois possíveis leitores a incorporar no projeto, que serão analisados de seguida na tabela 4.2.

Tabela 4.2: Especificações Técnicas do Leitor PN532 e do Leitor ACR122

[58] [59]

	Leitor PN532	**Leitor ACR122 USB**
Alcance de Leitura	até 10 cm	até 5 cm
Frequência	13.56 MHz	13.56 MHz
Formato dos Cartões	ISO/IEC 14443A, ISO/IEC 14443B, NFC e Felica	ISO/IEC 14443A, ISO/IEC 14443B, NFC e Felica
Anti-colisão	Sim	Sim
Interfaces	SPI, I2C ou *Serial UART*	USB ou RS232
Protocolos	SPI ou I2C	USB ou RS232
Velocidade de Comunicação	212 KBits/s ou 424 KBits/s	424 Kbits/s
Preço	44.22€[60]	47.80€[61]

Assim, depois de analisadas as características dos dois leitores, escolheu-se o leitor PN532 porque tem um alcance de leitura superior e tem um preço mais reduzido. De resto, ambos os leitores têm características semelhantes, permitindo os dois a sua ligação ao Raspberry Pi, visto que têm interfaces de ligação que o permitem. Na figura 4.1 é possível observar-se uma imagem ilustrativa do leitor escolhido: o leitor PN532.

[1] requisito definido em 3.1

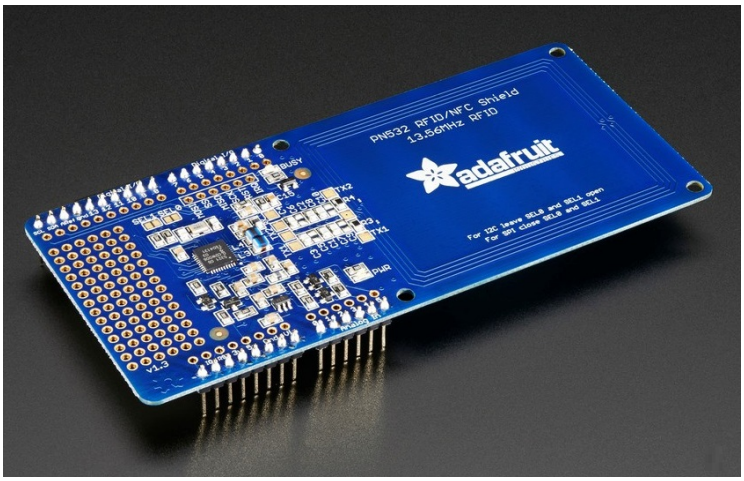


Figura 4.1: Ilustração do leitor PN532 [62]

Após a escolha do leitor de NFC, foi ainda necessário selecionar um modelo de cartões NFC que serão utilizados no processo de identificação. O cartão escolhido foi o "Cartão Ultralight Gloss", que funciona a 13.56 MHz e tem um tamanho standard [2], com um CHIP NXP Ultralight EV1. Na figura 4.2 encontra-se uma imagem ilustrativa dos cartões NFC escolhidos. [48]

Figura 4.2: Imagem ilustrativa do cartão NFC [63]

4.1.3 Leitor RFID

Procedeu-se a uma análise aos leitores já existentes no laboratório da FEUP, para se identificar qual o leitor RFID a utilizar, tendo como requisito suportar a leitura de várias etiquetas RFID em simultâneo.

Um dos leitores analisados foi o leitor PN532, já utilizado para a identificação de pessoas, também suporta a tecnologia RFID. As características gerais do leitor estão patentes na tabela 4.2.

Uma outra gama de leitores considerados foram o leitor ID-12 e o leitor ID-20, sendo que as suas especificações técnicas se encontram na tabela 4.3.

[2] tamanho de um cartão de crédito

Tabela 4.3: Especificações Técnicas do Leitor ID-12 e ID-20

[64] [65]

Alcance de Leitura	até 12 cm	até 18 cm
Frequência	125 KHz	125 KHz
Formato dos Cartões	EM4001	EM 4001
Interfaces	9600bps TTL e RS232	9600bps TTL e RS232
Anti-colisão	Não	Não
Preço	31.92€	36.84€

Na figura 4.3 é possível uma imagem ilustrativa do leitor ID-12.

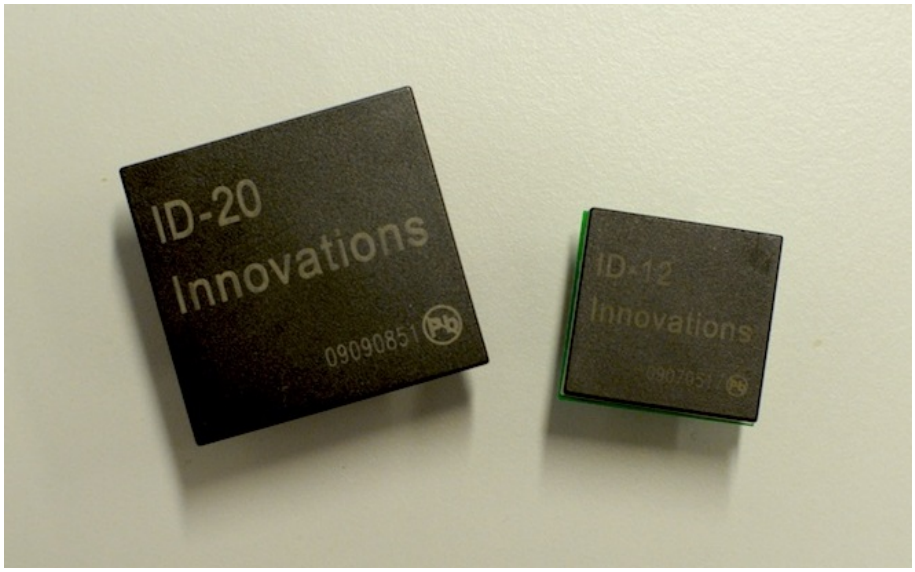


Figura 4.3: Ilustração do leitor ID-12 e do leitor ID-20 [66]

Por fim, ainda se analisou o leitor RFID ID ISC.PR101-A. As suas caraterísticas estão expostas na tabela 4.4.

Tabela 4.4: Especificações Técnicas do leitor ID ISC.PR101-A

[67] [68]

Alcance de Leitura	até 18 cm
Frequência	13.56 MHz
Tipo de etiqueta	passiva
Antena	Interna
Formato dos Cartões	ISO15693, ISO18000-3-Mode1
Interfaces	RS232 ou RS485
Anti-colisão	Sim
Preço	288.00€[69]

Na figura 4.4 é possível visualizar uma imagem ilustrativa do leitor ID ISC.PR101-A.

Figura 4.4: Ilustração do leitor ID ISC.PR101-A [67]

Após a análise dos leitores acima referidos e tendo os dois interfaces de comunicação que permitem a sua ligação ao Raspberry Pi, a escolha inicial foi o leitor ID-12 por se encontrar imediatamente disponível no stock do laboratório onde foi desenvolvida a dissertação. No entanto, não existia uma biblioteca que permitisse o uso do leitor em Linux. Tendo em consideração que o desenvolvimento manual da interface de software com o sistema operativo, era muito demorada e não correspondia aos objetivos deste projeto, optou-se por outro sensor que fosse compatível com o sistema operativo em uso. Neste sentido, foi escolhido o leitor RFID ID ISC.PR101-A, que estava disponível nos inventários de outro laboratório na FEUP. De notar que, embora seja mais caro, também oferece melhores garantias de funcionamento em situações de colisão de etiquetas RFID.

No caso da identificação de pessoas, situações de colisão de etiquetas NFC, poderão ser um fator pouco preocupante, visto que quando uma pessoa se estiver a identificar dificilmente mais alguém estará no alcance de leitura do leitor (10 cm). Contudo, no caso do leitor RFID, o risco de colisões de leituras simultâneas é muito maior, sendo que a escolha do leitor ID ISC.PR101-A permite que os utilizadores registem vários objetos simultaneamente, o que possibilita até a otimização de tempo no registo dos objetos.

4.2 Implementação do modelo cliente-servidor na plataforma computacional

Tal como abordado no terceiro capítulo, foi desenvolvido um sistema do tipo cliente-servidor em cada plataforma computacional. Cada plataforma computacional, tem instalado o *Raspbian*, sistema operativo *Linux*, sendo que a linguagem de programação escolhida para a implementação dos clientes leitores, sensores e atuadores foi o C++. Por outro lado, o servidor foi implementado através da linguagem C++, com SQL embebido em C++ para a consulta de dados na base de dados.

Do ponto de vista funcional, sempre que a plataforma computacional é ligada, é executado um

script responsável por iniciar todos os programas inerentes ao funcionamento do sistema implementado, ou seja, é iniciado o servidor, bem como todos os clientes do servidor.

A ligação entre o servidor e os clientes, foi assegurada com recurso à utilização de *sockets*, que são uma interface de comunicação entre processos. Nesta dissertação, implementou-se um servidor com *sockets* de domínio *AF_UNIX* e o tipo *SOCK_STREAM*, utilizados para a troca de dados entre processos que executam dentro da mesma plataforma computacional.

De forma a permitir a modularidade do sistema, o servidor implementado é multiprocessos, assim, quando o servidor é iniciado, fica à espera da ligação de novos clientes, sendo que sempre um cliente novo se liga ao servidor, é criado um novo processo, através da utilização de *threads*, para tratar a ligação efetuada. Deste modo, podemos ter vários clientes em simultâneo conetados ao servidor.

Na figura 4.5, é possível observar-se um exemplo de uma ligação entra um cliente e um servidor. Começando a análise na parte do servidor, este começa por iniciar um *socket* e fazer *bind* ao *socket*, por forma a dar-lhe um nome [70]. Posteriormente, o servidor executa a função *listen*, ficando à espera da ligação de novos clientes. Nesta fase, quando um novo cliente é criado, este inicia o *socket*, não necessitando de fazer *bind*, pois já foi efetuado pelo servidor. Depois da criação do *socket*, o cliente efetua um pedido para se ligar ao servidor, sendo que, quando este é aceite, o servidor responde-lhe a dizer que aceitou a conexão e procede há criação de uma *thread* que será a responsável pela manutenção da ligação com este cliente, usando uma outra porta. Após isto, o cliente e o servidor podem comunicar entre si, até que um deles seja desligado.

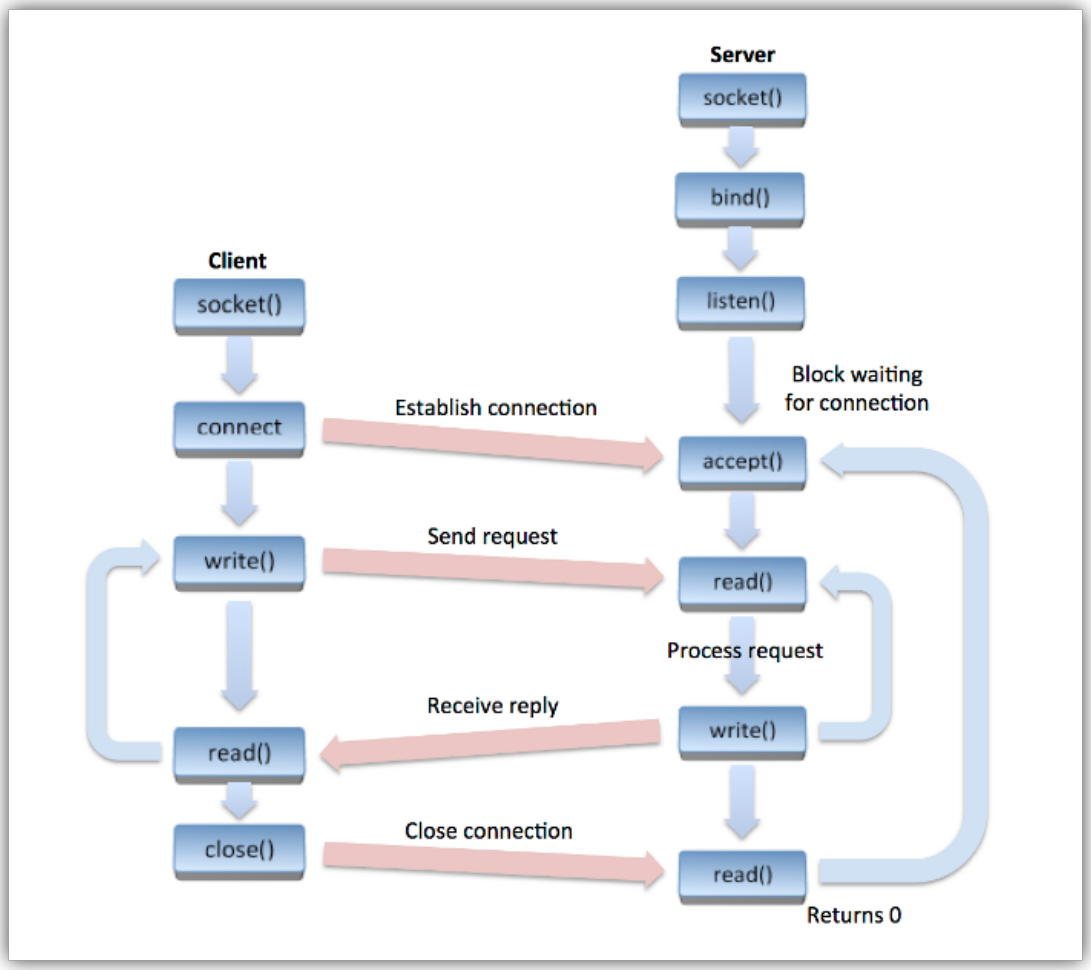


Figura 4.5: Ilustração da ligação de um cliente a um servidor [71]

Devido à arquitetura implementada, pode-se adicionar ou substituir os leitores, sensores ou atuadores [3] sem ser necessário modificações no servidor. Para isso, é necessário configurar um novo cliente, de acordo com o protocolo desenvolvido, visto que a gestão por parte do servidor mantém-se funcional.

Cada novo cliente será desenvolvido de raiz, de modo a garantir o correto funcionamento do leitor, sensor ou atuador. Por exemplo, um novo cliente responsável pela gestão de um leitor NFC terá de ser implementado de forma garantir a comunicação com o servidor, a obtenção das leituras e a construção e envio correto das tramas para o servidor. Além deste aspeto, para a configuração de novos clientes é ainda necessário atualizar o *script* de iniciação do servidor e dos clientes, executado sempre que se liga o Raspberry Pi.

Em termos de configurações genéricas, foi implementado no servidor, a leitura de um ficheiro de configuração do tipo .txt. Tal como se pode ver na figura 4.6, neste ficheiro está guardado o

[3] desde que existam portas de ligação disponíveis no Raspberry Pi

endereço IP do Raspberry Pi que aloja a base de dados, que neste caso é 192.168.105.1, e o número da bancada de laboratório onde será colocada a plataforma computacional, sendo que neste exemplo o ficheiro de configuração corresponde à bancada número 2. O número da bancada de laboratório é definido automaticamente após ser inserida uma nova bancada na base de dados, sendo que este pode ser depois consultado na página web implementada. O ficheiro de configuração é sempre definido manualmente quando se instala uma nova bancada.

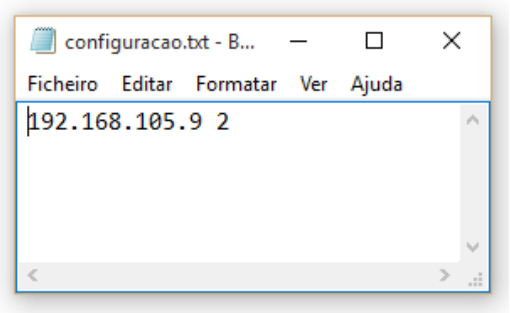


Figura 4.6: Ilustração do ficheiro de configuração

A comunicação entre o servidor e a base de dados é efetuada através da rede de área local existente no laboratório.

4.2.1 Protocolo desenvolvido

A transmissão de informação, quer entre os clientes e o servidor, quer entre o servidor e os clientes é feita através de um protocolo próprio, desenvolvido para garantir uma comunicação simples e eficaz entre os clientes e o servidor e vice-versa.

As tramas do protocolo implementado, são enviadas entre o servidor e um cliente, ou entre um cliente e o servidor, através de *strings* em C++.

Na tabela 4.5, podem-se observar os identificadores utilizados para enviar mensagens para o servidor por forma a identificar qual a origem da mensagem, isto é, se a informação é proveniente de um leitor, de um sensor ou de um atuador.

Tabela 4.5: Identificadores utilizados pelos clientes para envio de mensagens ao servidor

Identificador	**Cliente de origem da mensagem**
01	leitor NFC
10	leitor RFID
30	botão *shutdown* [4]
31	botão *logout* [4]
99	atuador Led's

[4] descrito em 4.2.4

Por outro lado, na tabela 4.6, podem-se observar os identificadores utilizados pelo servidor para enviar mensagens para o cliente atuadores, por forma a ativar algum atuador. De notar que existem 4 atuadores diferentes que indicaram estados básicos da bancada, sendo a sua descrição apresentada em 4.2.5.

Tabela 4.6: Identificadores utilizados pelo servidor para envio de mensagem aos clientes

Identificador	**Origem da mensagem**	**Destino da mensagem**
90	servidor	atuador led verde
91	servidor	atuador led amarelo 0
92	servidor	atuador led amarelo 1
93	servidor	atuador led vermelho

4.2.2 Cliente - Leitor NFC

O cliente responsável pelo leitor NFC tem como função iniciar o leitor e, posteriormente, sempre que uma etiqueta NFC é detetada, enviar uma trama para o servidor de acordo com o protocolo implementado. Na figura 4.7, pode-se visualizar uma trama do protocolo desenvolvido que contém o identificador *01*, indicando que se trata de um cliente - leitor NFC, com a informação de um -*Unique Identifier* - UID NFC - *c3d920d4*.

Figura 4.7: Imagem ilustrativa de um trama do protocolo desenvolvido enviada por um cliente - leitor NFC

A comunicação entre o leitor PN532 e o Raspberry Pi foi configurada através do protocolo *Inter-Integrated Communication* - I^2C. Para isso, foi necessário configurar as portas I^2C do Raspberry Pi. [72]

Para a implementação do cliente leitor NFC, foi instalada e utilizada a biblioteca *libnfc* em C++ [5]. Com o recurso à biblioteca referida, foi implementado um algoritmo em C++ [6] que efetua a leitura de etiquetas NFC que sigam a norma ISO/IEC 14443.

[5] disponibilizada online em [73]
[6] base do algoritmo implementado disponível em [74]

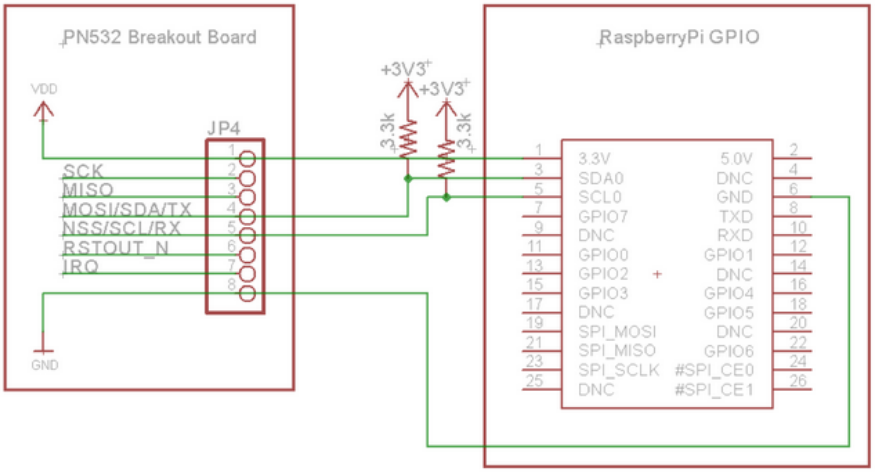


Figura 4.8: Esquema de ligação do leitor PN 532 ao Raspberry Pi [75]

O cliente responsável pelo leitor NFC funciona num ciclo infinito, em que sempre que deteta uma leitura de um UID NFC, este é enviado para o servidor, de acordo com o protocolo definido. Assim, cabe sempre ao servidor o tratamento da informação proveniente do leitor NFC, conforme o estado do sistema nessa altura. Ou seja, se um colaborador estiver a utilizar uma bancada e identificar-se perante o sistema, esta ação representará um *logout*, ao passo que se a bancada estiver livre e um colaborador se identificar perante o sistema, esta ação representará uma tentativa de *login*.

4.2.3 Cliente - Leitor RFID

O leitor RFID utilizado para a identificação de objetos é o leitor ID ISC.PR101-A. Na parte central do leitor existe um led multicor que indica um dos três estados possíveis:

- cor de laranja - quando o leitor está a iniciar;
- verde - leitor ligado, sem detetar etiqueta(s) RFID;
- vermelho - leitor e ler etiqueta(s) RFID.

Dependendo da configuração, a transmissão de dados entre o leitor e o *host* [7] pode ser efetuada de dois modos distintos, sendo eles: *ISO Host Comands* e *Scan Mode*. Para esta dissertação, foi escolhido o modo de funcionamento *Scan Mode*, que consiste no envio do UID da etiqueta RFID para o *host*, sempre que uma etiqueta RFID esteja presenta na zona de leitura. No caso de várias etiquetas RFID serem lidas pelo leitor, serão enviados para o *host* todos os UID lidos pelo leitor.

O leitor RFID foi ligado ao *host*, que neste projeto é o Raspberry Pi, através da porta UART (*Universal Asynchronous Receiver/Transmitter*) utilizando o protocolo RS232, também denominado como porta série. Dado que o leitor ID ISC.PR101-A funciona a uma tensão de 15 Volts, dorante V, mas a porta UART do Raspberry Pi funciona a 3.3V foi necessário utilizar um MAX3232,

[7] dispositivo ao qual o leitor se encontra ligado

de acordo com o esquema de ligações ilustrado na figura 4.9, para converter os sinais recebidos do leitor para sinais com níveis de tensão que o Raspberry Pi pudesse receber com segurança.

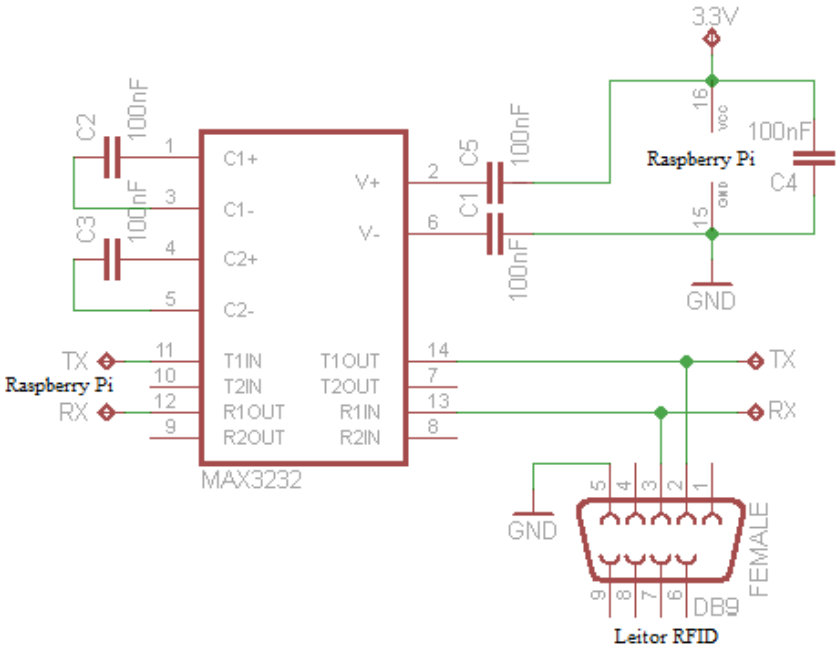


Figura 4.9: Esquema de ligações do MAX3232 ao Raspberry Pi e ao leitor RFID [76]

O Raspberry Pi executa o *Raspbian*, sendo que neste a porta série é utilizada por defeito pela consola do sistema. Dado que o leitor RFID tem como interface de comunicação o protocolo RS232, foi necessário configurar a porta série do Raspberry Pi de modo a permitir que seja utilizada por qualquer programa executado pelo Raspberry Pi e não apenas pela consola do sistema, como estava definido por defeito. Deste modo, o *Raspbian*, foi configurado para permitir que os sinais recebidos pela porta série, ficassem visíveis pelo sistema operativo no ficheiro especial */dev/ttyAMA0* [8]. [77] [78]

Após a configuração acima referida, foi necessário definir as configurações no programa que é responsável pelo leitor RFID. Assim, as configurações foram feitas de acordo com a programação do leitor e as especificações da porta série do Raspberry Pi, isto é, a *baud rate* [9] foi defina igual à *baud rate* do leitor RFID e o *modem device* no programa foi definido para enviar os UID das etiquetas RFID lidas pelo leitor para o ficheiro *dev/ttyAMA0* do Raspberry Pi. O programa desenvolvido teve por base a utilização da biblioteca *termios.h*, bem como o exemplo disponibilizado em [79], para a leitura de dados no Raspberry Pi via porta série.

No desenvolvimento desta dissertação, e para efeitos de testes ao sistema implementado, foram utilizadas umas etiquetas RFID da *Texas Instruments* com o modelo *Tag-it HF-I Plus*. Estas etiquetas, que se podem observar na figura 4.10, foram desenvolvidas de acordo com as normas

[8] ficheiro do sistema que guarda os dados lido pela porta série
[9] define a velocidade do protocolo de comunicação RS232

ISO/IEC 15693 e ISO/IEC 18000-3 [80]. Assim, para os casos de aplicações reais deste sistema, as etiquetas RFID utilizadas têm cumprir as referidas normas para serem detetadas pelo sistema.

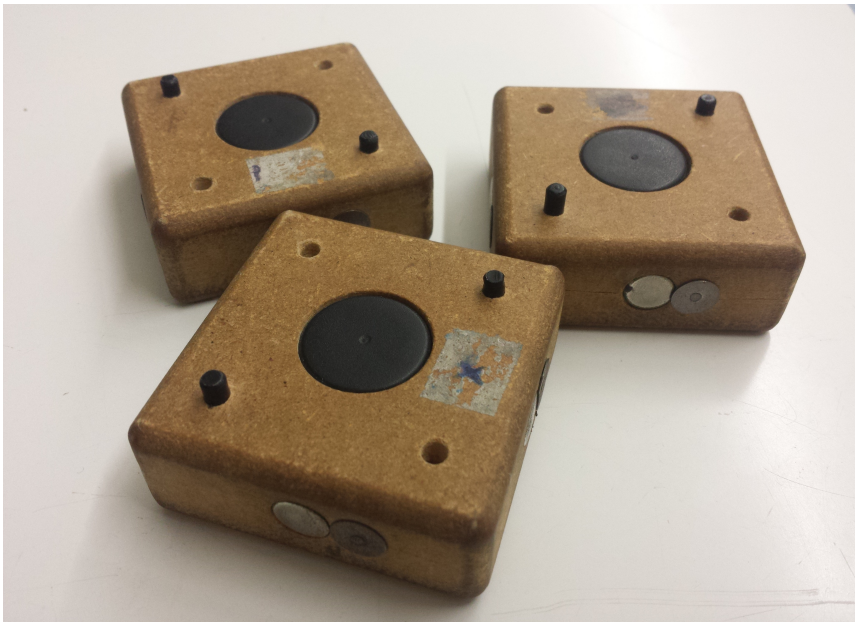


Figura 4.10: Ilustração de 3 etiquetas RFID utilizadas

O cliente responsável pelo leitor RFID funciona num ciclo infinito, sendo que quando é efetuada uma leitura de um UID RFID, esta é enviada para o servidor, respeitando o protocolo definido. Na figura 3.4, pode-se observar o exemplo de uma trama com o idnetificador de um leitor RFID - *10* e a informação de um UID RFID - *E00780ACDDE83275*.

4.2.4 Cliente - Botões

No desenvolvimento do sistema foram utilizados dois botões de pressão: um para desligar todo o sistema, doravante botão *shutdown* e o outro para registar o *logout* dos colaboradores.

A base da implementação dos programas C++ que detetam o estado do botão correspondente a cada um deles foi a mesma, sendo que a diferença entre os dois programas está apenas na trama que é enviada para o servidor, de acordo com o descrito na tabela 4.5. Deste modo, é executado em ciclo infinito um programa que lê o estado do botão, sendo que sempre que o botão é premido, o programa cria uma trama, enviando-a ao servidor por forma a informá-lo da ação detetada.

Nesta dissertação foram implementados dois clientes com base em botões de pressão, no entanto, estes podem ser substituídos por outro tipo de sensores, desde que tenham compatibilidade com as portas I/O livres do Raspberry Pi e respeitem o protocolo implementado.

Figura 4.11: Ilustração de um botão de pressão [81]

4.2.5 Cliente - Atuadores Led's

Os atuadores utilizados no desenvolvimento da dissertação foram led's, porque apenas é necessário simular os estados básicos da bancada como por exemplo, se está operacional ou se alguém a está a utilizar.

Para o controlo do estado dos led's, o programa desenvolvido utilizou a biblioteca *pigpio.h* [10]. Para isso, foi necessário a instalação da biblioteca no Raspberry Pi. Após isso, foi desenvolvido o programa, sendo que no início envia uma trama para o servidor para o informar que os atuadores estão ligados, e depois, executa um conjunto de operações em ciclo infinito. Este conjunto de operações consiste em esperar pelo receção de tramas provenientes do servidor e proceder à ativação, ou desativação, da porta onde está ligado o led em questão, dependendo do conteúdo da trama e tendo em conta os identificadores referidos na tabela 4.6. Assim, a informação que uma dada trama tem proveniente do servidor é um de dois estados possíveis:

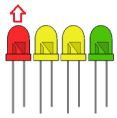
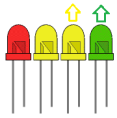
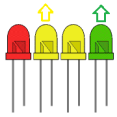
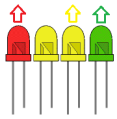
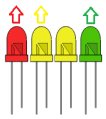
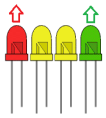
- **0** - para desligar o led em questão;
- **1** - para ligar o led em questão.

De seguida é apresenta na tabela 4.7 um conjunto de estados possíveis dos led's [11], com a descrição do significado de cada um destes estados.

[10] disponível em [82]

[11] led ligado representado com uma seta em cima

Tabela 4.7: Tabela com descrição do estado dos led's

Estado do sistema	**Estado dos led's**
Bancada laboratorial inoperacional.	
Bancada laboratorial livre. Para registar um *login* utilizar leitor NFC.	
Bancada laboratorial com *login* ativo. Lê e guarda etiquetas RFID.	
Bancada laboratorial livre e sem tentativas de registo ou com tentativa de registo com etiqueta NFC desconhecida pela base de dados. Para registar um *login* utilizar leitor NFC.	
Bancada laboratorial com *login* ativo, mas cujo tempo de reserva da bancada foi ultrapassado. Lê e guarda etiquetas RFID até ser efetuado um *logout*.	
Bancada laboratorial livre, após uma utilização por parte de algum colaborador. Para registar um *login* utilizar leitor NFC.	

4.2.6 Servidor

O esquema de funcionamento do servidor desenvolvido no âmbito desta dissertação, pode ser observado na figura 4.12. Nesta é visível que, após servidor ser iniciado, existe a verificação do estado da bancada de laboratório, isto é, se está operacional ou, se por algum motivo, está inoperacional. Esta verificação, à semelhança de todos os acessos feitos à base de dados, é efetuada através de uma query SQL embebida em C++ enviada à base de dados, sendo que mediante o resultado da query, o servidor conseguirá saber o estado da bancada.

Se o estado for inoperacional, será envida uma trama ao cliente atuadores de modo a ligar o led vermelho e fica a aguardar o recebimento de uma trama. Quando uma trama é recebida, o ser-

vidor verificará se a trama é proveniente do cliente atuador responsável por desligar a plataforma computacional da bancada laboratorial. No caso de ser, o Raspberry Pi é desligado, no caso de não ser, o servidor ignora o conteúdo da trama recebida e continua a receber tramas, até ser desligado. No entanto, se o estado da bancada for operacional, o resto das operações efetuadas pelo servidor, serão descritas abaixo.

Quando uma trama é recebida, o servidor divide-a nas suas duas componentes: identificador e informação. Deste modo, o servidor consegue saber qual o tipo de informação recebida devido ao identificador, tratando-a de forma conveniente.

Se o identificador recebido corresponder a um cliente leitor NFC, o servidor efetuará um, de dois, procedimentos:

- caso exista um *login* efetuado, o servidor não irá utilizar o UID NFC recebido para nada. O servidor tem uma variável auxiliar que lhe indica se existe um *login* ativo ('1') ou não ('0').
- caso não exista um *login* efetuado, o servidor irá utilizar o UID NFC recebido para verificar se é conhecido pela base de dados;
    1. se for conhecido irá verificar se existe alguma reserva efetuada para aquela hora na bancada de laboratório em que se está a autenticar;
        (a) se existir uma reserva naquela hora é efetuado o login e o servidor enviará quatro tramas para o cliente atuadores, mudando o estado dos led's: ativando o led verde e o led amarelo 1 e desativando o led amarelo 0 e vermelho;
        (b) se não existir uma reserva naquela hora, o servidor aguardará até receber uma nova trama, e enviará duas tramas ao cliente atuadores, uma para ligar o led amarelo 0 e outra para desligar o led vermelho;
    2. se não foi conhecido, o servidor aguardará até receber uma nova trama com um novo identificador NFC, e enviará duas tramas ao cliente atuadores, uma para ligar o led amarelo 0 e outra para ligar o led vermelho;

No caso do identificador recebido pelo servidor indicar que se trata de um cliente leitor RFID, este irá:

- se não existir um login efetuado, continuar a receber tramas, não guardando o UID RFID recebido.
- se existir um login efetuado na bancada, o servidor irá verificar se o UID RFID pertence a algum dos objetos registados na base de dados. Para casos em que pertença, o UID RFID é registado na base de dados, porque o objeto é conhecido pelo sistema, caso contrário este não é registado na base de dados. Desta forma, é criado um histórico dos objetos utilizados em cada operação numa bancada. No caso do servidor receber duas, ou mais, vezes o mesmo UID RFID de um objeto conhecido, este só será registado uma vez na base de dados.

Por outro lado, quando o servidor deteta que recebeu um identificador correspondente a um dos botões irá agir em conformidade:

- se recebeu uma trama proveniente do botão *shutdown* irá registar o *logout* do utilizador, e desligar o sistema de seguida.
- se recebeu uma trama proveniente do botão *logout*:

  - e existir um colaborador com *login* efetuado: irá registar o *logout* do utilizador, e enviar duas tramas para o cliente atuadores por forma a ligar os led's verde e amarelo 0;
  - se não existir um colaborador com *login* efetuado, irá aguardar até receber uma nova trama.

No caso de um utilizador exceder o tempo da reserva que tinha feito para a bancada, o servidor, que executa um algoritmo em ciclo infinito, poderá efetuar uma das duas situações abaixo descritas:

- logout automático por parte do servidor, registando-o na base de dados e informando o colaborador através do envio de uma trama para o cliente atuadores, ativando o led vermelho e o led verde, sendo que o led amarelo 1 será desativado.
- informar o colaborador que o tempo da sua reserva acabou, através do envio de uma trama para o cliente atuadores, ativando o led vermelho. Neste caso, o colaborador saberá que o seu tempo de reserva da bancada expirou pois tem o led verde, amarelo 1 e vermelho ligados. No entanto, poderá continuar a utilizar a bancada e registar objetos, até que seja detetada uma reserva para o minuto seguinte, sendo que aí o servidor efetuará o descrito acima no ponto 1.

Por fim, se o servidor receber uma trama com o identificador cliente atuadores, situação que ocorre apenas quando todo o sistema é ligado, o servidor irá enviar uma trama para o cliente atuadores por forma a ligar os led's verde e vermelho, indicando assim que o sistema está inicializado.

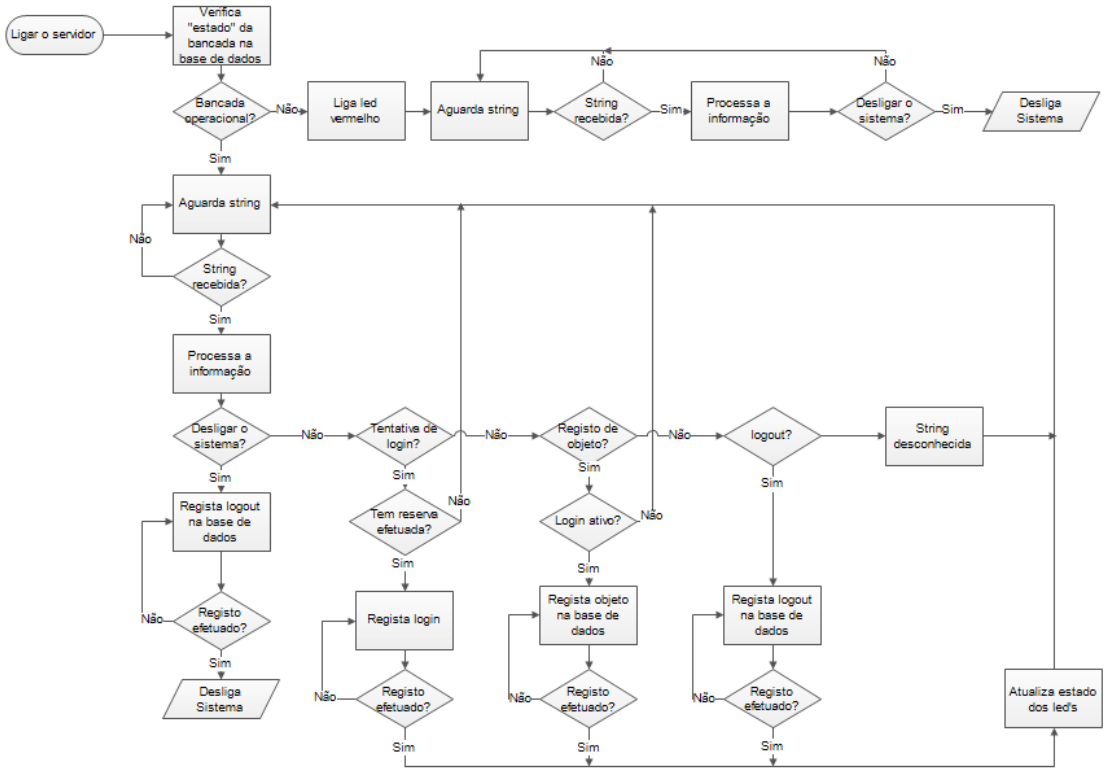


Figura 4.12: Esquema ilustrativo do funcionamento do servidor

Como já referido, o servidor acede sempre à base de dados através do envio de query's SQL embebidas em C++. Após a ligação à base de dados e processamento da query, a base de dados envia um query de resposta, podendo o servidor continuar o seu normal funcionamento de acordo com o ilustrado na figura 4.12.

Na figura 4.13, podem-se observar os leitores, sensores e atuadores conetados ao Raspberry Pi. Esta representação ilustra uma bancada de laboratório, sendo que os números a observar na figura representam:

1. led's utilizados para simular os atuadores;
2. botões que permitiram simular os sensores;
3. leitor NFC e cartões NFC;
4. leitor RFID e etiquetas RFID;
5. raspberry pi que aloja o servidor com as ligações aos diversos clientes.

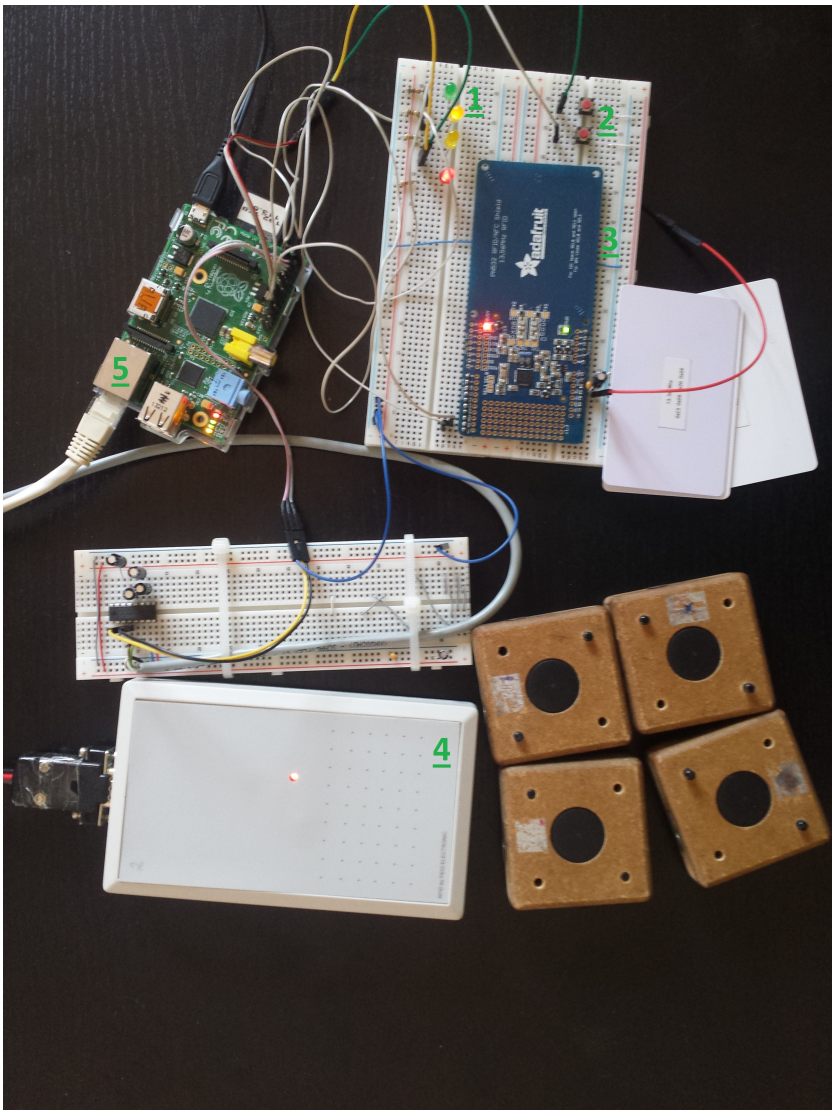


Figura 4.13: Representação ilustrativa de bancada laboratorial com leitores, sensores e atuadores

4.3 Interface de gestão e histórico da utilização das bancadas de laboratório

Para o desenvolvimento da interface web, foi necessário instalar um conjunto de *software* de código aberto, denominado LAMP [12] de modo a permitir a implementação da base de dados e da página web. [83]

4.3.1 Base de dados

A base de dados foi implementada através de um servidor mysql no Raspberry Pi da *bancada laboratorial -servidor*, visto que estará sempre ligada, permitindo assim que a base de dados esteja

[12] sigla - Linux, Apache, MySQL e PHP

sempre acessível. Após a instalação do servidor mysql, foi também instalado um *package* que permite a utilização da linguagem php [13] para aceder à base de dados.

De seguida, foi criado um utilizador com permissões totais no acesso à base de dados, isto é, o utilizador criado pode efetuar todo o tipo de alterações na base de dados, desde criação/eliminação de tabelas até consultas, inserção ou eliminação de dados na base de dados. Este utilizador, será partilhado por todos os servidores instalados nos Raspberry's Pi nas bancadas de laboratório, porque na configuração da base de dados não foi definido um número máximo de ligações à base de dados, permitindo assim, que o mesmo utilizador aceda de diversos clientes simultaneamente e faça alterações na base de dados. [84]

A base de dados foi implementada em linguagem sql, de acordo com o modelo relacional presente na figura 3.5.

Foi ainda instalado nos Raspberry Pi o phpmyadmin, que é uma página web em php que permite uma fácil administração de bases de dados. Deste modo, é possível aceder à base de dados do Raspberry Pi principal através de um *browser* desde que se conheça o seu endereço IP.

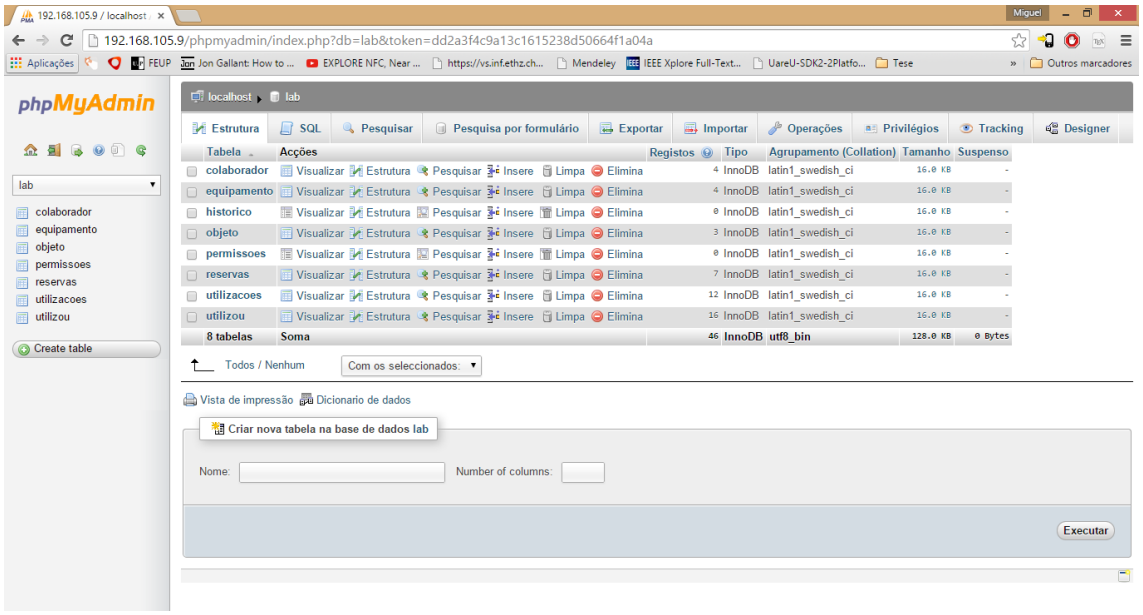


Figura 4.14: Base de dados implementada vista num *browser* com recurso ao phpmyadmin

4.3.2 Página web

A página web foi implementada nas linguagens *HyperText Markup Language* -HTML, *Hypertext Preprocessor* -PHP e Javascript, sendo que o *design* foi desenvolvido em CSS -*Cascading Style Sheets*. O HTML é uma linguagem de programação utilizada para conceber páginas web estáticas, ou seja, que só apresentam informação armazenada no servidor que aloja a página. Por

[13] utilizada para implementar a página web

outro lado, o PHP permite desenvolver páginas web dinâmicas e aceder a bases de dados. O Javascript foi utilizado para fornecer avisos aos utilizares da página, através de janelas *pop-up*. Na página web desenvolvida, estas janelas foram utilizadas para informar os colaboradores de uma resposta a um pedido seu, como por exemplo, se a reserva de uma bancada de laboratório foi efetuada com sucesso, sendo necessário que o utilizador feche a referida janela, para conseguir continuar a utilizar a página web. [85] [86]

O *template* desenvolvido é do tipo responsivo, de modo a otimizar as funcionalidades da página conforme os acessos sejam feitos através de *smartphones*, *tablets* ou computadores.

Do ponto de vista do alojamento da página web, foi necessário dar permissões de escrita no diretório "/var/www"do Raspberry Pi, de modo a permitir que se inserissem os ficheiros HTML, PHP, Javascript e CSS naquele diretório, que é onde a página web está alojada. [87]

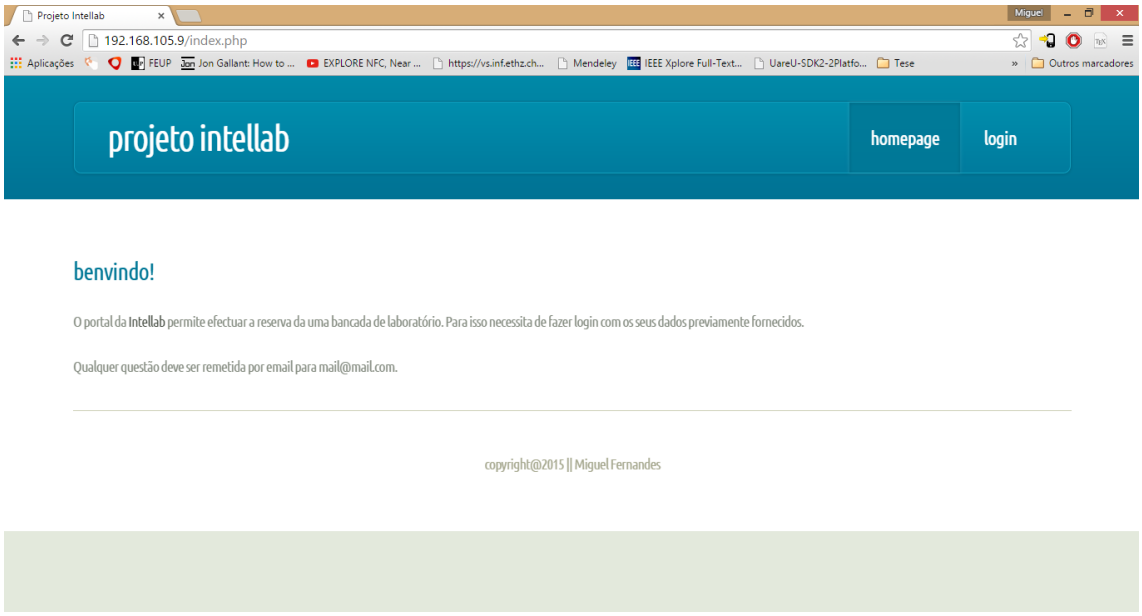
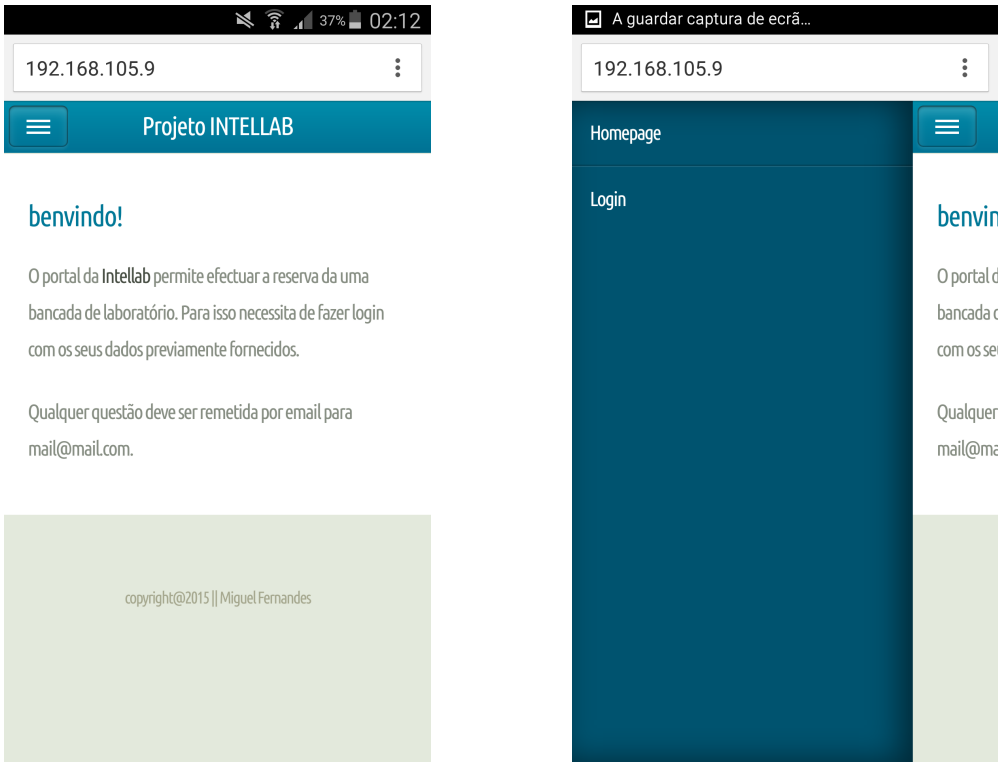


Figura 4.15: Visualização da página web implementada obtida através da captura de ecrã do computador



(a) Página inicial.

(b) Menu [a].

[a] sem *login* efetuado

Figura 4.16: Visualização da página web implementada obtida através da captura de ecrã de *smartphone*

A página web foi desenvolvida de modo a cumprir todos os requisitios definidos em 3.1. Nesse sentido a página foi implementada tendo em conta os dois tipos de utilizadores: o administrador do sistema e os colaboradores. Para a utilização da página web é necessário ser efetuado um *login*, caso contrário apenas é disponibilizada informação genérica acerca do sistema e, claro, um campo onde é possível efetuar a autenticação na página.

O primeiro administrador do sistema será sempre a pessoa cujos dados tiverem sido inseridos em primeiro lugar na base de dados, podendo posteriormente ser nomeados mais administradores para o sistema. Deste modo, o *login* do administrador do sistema pode ser gerado antes da instalação do sistema num laboratório e depois disponibilizado ao cliente final, ou então, pode ser gerado à *posteriori*. Neste caso, o administrador do sistema terá de aceder à base de dados através de um *browser*, sendo que o *Uniform Resource Locator*- URL a inserir será: "*ip*/phpmyadmin", onde *ip* deve ser substituído pelo IP do Raspberry Pi que aloja a base de dados. Após isto, terá de se autenticar na base de dados e poderá proceder ao registo do administrador do sistema.

Por outro lado, no caso do *login* dos colaboradores, o *username* é definido pelo administrador do sistema, aquando do registo de um colaborador na interface web, e a *password* é gerada automaticamente pela base de dados, sendo os dados entregues ao colaborador pelo administrador do sistema ou outra pessoa que tenha sido indicada para o efeito. Em ambos os casos, é possível trocar a qualquer momento as *passwords* na interface web.

O administrador do sistema, poderá ainda nomear outros colaboradores como administradores do sistema. Contudo, a página web não permitirá que os colaboradores promovidos a administradores do sistema retirem a permissão de administrador à primeira pessoa que tenha sido registada na base da dados. Ou seja, esta pessoa será sempre administradora do sistema, podendo nomear outras, mas nunca poderá sair de administrador, ao passo que todos os outros podem sair de administradores.

Por fim, os administradores do sistema podem definir permissões de utilização das bancadas aos colaboradores. Desta forma, é possível que os colaboradores não tenham permissões de utilização em todas as bancadas laboratoriais, sendo que só podem efetuar reservas nas bancadas em que tiverem permissões de utilização.

Após uma autenticação bem sucedida na página, o menu gerado depende do tipo de utilizador que efetuou o *login*. Nesse sentido, de seguida serão explicadas as caraterísticas da interface web para os dois tipos de utilizadores.

4.3.2.1 Administrador do Sistema

Tal como se pode observar na fig 4.17, o menu foi desenvolvido para o administrador do sistema de modo a permitir-lhe efetuar um conjunto de ações, nomeadamente:

1. "Homepage- visualizar a sua informação pessoal e alterar a sua *password* pessoal;
2. "Histórico- visualizar o histórico de todos os colaboradores;
3. "Colaboradores- registar novos colaboradores, bem como associar um identificador NFC a um colaborador ou mesmo substituí-lo por outro. Nomear novos administradores para

o sistema. Remover administradores do sistema. Dar/retirar permissões de utilização nas bancadas laboratoriais;

4. "Objetos- inserir novos objetos na base de dados e associar a respetiva etiqueta ao objeto;
5. "Equipamento- incluir novas bancadas de laboratório na base de dados, bem como definir se uma dada bancada está operacional ou não;
6. "Agenda- aceder ao registo das reversas efetuadas e efetuar reservas de bancadas laboratoriais em seu nome.

Figura 4.17: Visualização do menu da página web para o administrador do sistema obtido através da captura de ecrã de *smartphone*

4.3.2.2 Colaboradores

A interface desenvolvida para os colaboradores, tal como se pode observar na fig 4.18, tem as seguintes funcionalidades:

1. "Homepage- visualizar a sua informação pessoal e alterar a sua *password* pessoal;
2. "Histórico- visualizar o seu histórico de utilizações das bancadas de laboratório;
3. "Agenda- aceder ao registo das reversas efetuadas e efetuar reservas de bancadas laboratoriais.

Figura 4.18: Visualização do menu da página web para os colaboradores do sistema obtido através da captura de ecrã de *smartphone*

Após a apresentação das funcionalidades implementadas na interface web, é ainda necessário clarificar que as reservas de bancadas só podiam ser feitas entre as 8:00 horas e as 20:00 horas durante todos os dias da semana, correspondendo ao horário de funcionamento do laboratório. De notar que a interface web não permite reservas sobrepostas para numa bancada, nem que um colaborador efetue reservas de forma simultânea em várias bancadas.

4.3.3 Capacidade de armazenamento de informação

A solução implementada tem limites ao nível da memória disponível para armazenamento da informação. No desenvolvimento desta dissertação foi utilizado um cartão de memória com capacidade de armazenamento de 8 GB. Para casos em que 8 GB se revelem insuficientes, poderá escolher-se um cartão de memória com maior capacidade ou então instalar a base de dados num servidor com mais memória. Neste caso, seria necessário redirecionar as ligações que são feitas à base de dados para esse novo servidor.

Capítulo 5

Principais Conclusões e Possíveis Trabalhos Futuros

5.1 Principais Conclusões

O desenvolvimento desta dissertação, que inicialmente previa um sistema de identificação de objetos e pessoas para uma única bancada laboratorial, culminou com um sistema de gestão de objetos e pessoas que utilizam as diversas bancadas laboratoriais existentes num laboratório.

Numa fase inicial do projeto, definiu-se uma arquitetura para o sistema, que satisfizesse todos os requisitos propostos. A arquitetura proposta permite que o sistema desenvolvido seja implementado em laboratórios com diferentes números de bancadas, porque encara cada bancada como um novo módulo do sistema. Este módulo para cada bancada é composto por uma plataforma computacional (Raspberry Pi) capaz de garantir a gestão dos leitores NFC e RFID, atuadores e sensores existentes na bancada.

Para cada bancada laboratorial, foi também definida uma arquitetura capaz de assegurar os requisitos propostos, nomeadamente a substituição, ou aumento, de leitores NFC ou RFID. Nesse sentido, foi decidido implementar um modelo do tipo cliente-servidor em cada plataforma computacional, sendo que o servidor é responsável por processar a informação proveniente dos clientes e comunicar com a base de dados do sistema, ao passo que os clientes são responsáveis pela gestão dos leitores, sensores e atuadores, conforme o caso. A comunicação entre o servidor e os clientes foi assegurada através do uso de *sockets*.

Por fim, e de acordo com os requisitos do sistema, foram especificadas as funcionalidades da interface web a ser desenvolvida, bem como desenhada uma base de dados para suporte ao sistema. Esta base de dados guarda toda a informação relevante para o seu funcionamento. Após a validação da arquitetura proposta passou-se à fase de implementação.

A fase de implementação foi a mais morosa. Inicialmente foi necessário estudar o modo de funcionamento dos leitores RFID e NFC, e, posteriormente, validar o seu correto funcionamento em conjunto com o Raspberry Pi.

De seguida implementou-se a base de dados, a página web e a arquitetura cliente-servidor no Raspberry Pi para a gestão dos leitores, atuadores e sensores. No final, foi necessário simular o correto funcionamento do sistema. Para isso, foi implementada a arquitetura cliente-servidor num outro Raspberry Pi, podendo assim simular-se novas bancadas de laboratório.

Nesta fase foram também efetuados testes funcionais à página web, como por exemplo o registo de colaboradores, objetos ou nova bancada, reserva da bancadas ou consulta do histórico de utilizações. Os testes realizados ao funcionamento das bancadas e da página web, permitiram concluir que o sistema se encontrava funcional.

Em suma, pode-se concluir que os objetivos propostos no início desta dissertação foram alcançados com sucesso.

5.2 Possíveis Trabalhos Futuros

O sistema de gestão de acessos às bancadas de laboratórios criado necessita que sejam feitas configurações iniciais em cada módulo, sempre que se acrescente uma nova bancada. Além disto, o sistema só tem um tipo de tecnologia para a identificação de pessoas e outro para a identificação de objetos.

Deste modo, poderão ser acrescentadas novas funcionalidades ao trabalho desenvolvido como por exemplo:

- implementação de algoritmo de pesquisa de rede, com o objetivo de "descobrir" todas as bancadas que estão ligadas à rede local. Deste modo, as bancadas cliente ligar-se-iam à bancada servidor através de uma configuração dinâmica, em detrimento da configuração estática implementada;
- dotar o sistema de novos tipos de identificação de pessoas, como por exemplo através da impressão digital, reconhecimento facial ou reconhecimento pela da retina dos olhos;
- replicação da base de dados;
- acrescentar um ecrã a cada plataforma computacional onde estivessem visíveis informações úteis como: a hora atual, as próximas reservas na bancada ou, no caso de uma bancada que esteja a ser utilizada, o tempo que falta para expirar a reserva da bancada;
- introduzir uma balança em cada bancada para o registo do peso dos objetos que foram utilizados; desde modo poder-se-ia determinar quais as quantidades de consumíveis que foram utilizados em cada trabalho;
- criação de um sistema de alertas para a necessidade de manutenção das bancadas; por exemplo, se um filtro de uma hotte química só tem 100 horas para correto funcionamento, quando as 100 horas fossem alcançadas o sistema emitiria um alerta automático para o administrador do sistema;
- incorporação do trabalho em bancada laboratorial, e desenvolvimento de soluções para garantir que o *hardware* que compõe o trabalho desenvolvido possa ser utilizado nos ambientes hostis de laboratório, como por exemplo, funcionar de forma eficaz, mesmo em contacto com ácidos.

Bibliografia

[1] "APRESENTAÇÃO | Laborial – Laboratory Solutions." [Online]. Disponível: http://www.laborial.com/?cat=4 [Acessido a: 2015-06-12]

[2] "Manual de Segurança Biológica. Instituto de Higiene e Medicina Tropical da Universidade Nova de Lisboa." [Online]. Disponível: http://www.ihmt.unl.pt/docs/Manual-de-Seguranca-Biologica.pdf [Acessido a: 2015-06-12]

[3] "Mobiliário Técnico Para Laboratorios." [Online]. Disponível: http://www.laborial.com/mobiliario-tecnico-para-laboratorios.html#tipologias [Acessido a: 2015-08-12]

[4] "Linha Blau | Laborial – Laboratory Solutions." [Online]. Disponível: http://www.laborial.com/?cat=10&linha=195 [Acessido a: 2015-06-13]

[5] "Linha Ahmar| Laborial – Laboratory Solutions." [Online]. Disponível: http://www.laborial.com/index.php?cat=10&linha=194 [Acessido a: 2015-06-13]

[6] "Linha Ahmar| Laborial." [Online]. Disponível: http://www.laborial.com/hottes-de-quimica.html [Acessido a: 2015-10-02]

[7] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*. John Wiley & Sons, 2010, vol. 4. [Online]. Disponível: https://books.google.com/books?id=jAszZEQYa9wC&pgis=1

[8] "Automatic Optical Character Recognition." [Online]. Disponível: https://www.linkedin.com/pulse/20140622192720-93747475-this-machine-will-replace-your-accountants [Acessido a: 2015-06-17]

[9] "Scanner OCR." [Online]. Disponível: https://upload.wikimedia.org/wikipedia/ar/7/70/Scanner_text.jpg [Acessido a: 2015-06-17]

[10] "Barcode – Barcoding News." [Online]. Disponível: http://www.barcodesinc.com/news/?tag=barcode [Acessido a: 2015-06-15]

[11] "Códigos bidimensionais | 2D |." [Online]. Disponível: http://www.oxxcode.com.br/codigo-datamatrix-2d/ [Acessido a: 2015-08-28]

[12] "Entenda o código de barras - PROTESTE - Associação de Consumidores." [Online]. Disponível: http://www.proteste.org.br/familia/nc/noticia/entenda-o-codigo-de-barras [Acessido a: 2015-06-16]

[13] "O primeiro código QR feito em calçada portuguesa." [Online]. Disponível: http://p3.publico.pt/vicios/hightech/4274/o-primeiro-codigo-qr-feito-em-calcada-portuguesa [Acessido a: 2015-06-16]

[14] "QR Code na calçada do Chiado." [Online]. Disponível: http://www.dinheirovivo.pt/buzz/interior.aspx?content_id=3876720 [Acessido a: 2015-06-16]

[15] "QR Code Marketing | Erica Marques." [Online]. Disponível: http://blog.ericamarques.com/2012/10/qr-code-marketing.html [Acessido a: 2015-06-16]

[16] "Smart card icons." [Online]. Disponível: http://stef.thewalter.net/smart-card-icons.html [Acessido a: 2015-06-15]

[17] "Kit Leitor GemPC Twin TR + Smart Card eCPF e eCNPJ :: Preço Baixo, Qualidade e Segurança." [Online]. Disponível: http://2kinformatica.webnode.com.br/products/produto-1/ [Acessido a: 2015-06-15]

[18] "Biometria." [Online]. Disponível: http://www.dicionarioinformal.com.br/biometria/ [Acessido a: 2015-06-15]

[19] "Sinfic SA." [Online]. Disponível: http://www.sinfic.pt/SinficWeb/displayconteudo.do2?numero=24095 [Acessido a: 2015-06-15]

[20] "Leitor Rfid Proximidade Mifare Usb - R$ 130,00 no MercadoLivre." [Online]. Disponível: http://produto.mercadolivre.com.br/MLB-663252528-leitor-rfid-proximidade-mifare-usb-_JM [Acessido a: 2015-06-15]

[21] "RFID History & Standards." [Online]. Disponível: http://www.fp7-aspire.eu/rfid/ [Acessido a: 2015-06-16]

[22] "RFID, Rádio Frequência ou Proximidade - Soluções Idonic." [Online]. Disponível: http://www.idonic.com/index.php?id=337 [Acessido a: 2015-06-16]

[23] "RFID - Identificação Rádio Frequência." [Online]. Disponível: http://www.gta.ufrj.br/grad/12_1/rfid/links/modos_de_comunicacao.html [Acessido a: 2015-02-26]

[24] "HDX and FDX : Oregon RFID." [Online]. Disponível: http://www.oregonrfid.com/index.php?main_page=page&id=31 [Acessido a: 2015-02-26]

[25] "About ISO - ISO." [Online]. Disponível: http://www.iso.org/iso/home/about.htm?= [Acessido a: 2015-06-15]

[26] "Padronização de Protocolos de RFID." [Online]. Disponível: http://www.teleco.com.br/tutoriais/tutorialrfid/pagina_3.asp [Acessido a: 2015-06-16]

[27] "ISO/IEC 18000-4:2008 - Information technology – Radio frequency identification for item management – Part 4: Parameters for air interface communications at 2,45 GHz." [Online]. Disponível: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46148 [Acessido a: 2015-06-16]

[28] "ISO/IEC 15963:2009 - Information technology – Radio frequency identification for item management – Unique identification for RF tags." [Online]. Disponível: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=52124 [Acessido a: 2015-06-16]

[29] "ISO 11784:1996 - Radio frequency identification of animals – Code structure." [Online]. Disponível: http://www.iso.org/iso/catalogue_detail?csnumber=25881 [Acessido a: 2015-09-03]

[30] "ISO 11785:1996 - Radio frequency identification of animals – Technical concept." [Online]. Disponível: http://www.iso.org/iso/catalogue_detail?csnumber=19982 [Acessido a: 2015-09-03]

[31] "ISO/IEC 14443-1:2013 - Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics." [Online]. Disponível: http://www.iso.org/iso/catalogue_detail.htm?csnumber=39693 [Acessido a: 2015-09-03]

[32] "ISO/IEC 14443-2:2010 - Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2: Radio frequency power and signal interface." [Online]. Disponível: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50941 [Acessido a: 2015-09-03]

[33] "ISO/IEC 14443-3:2011 - Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision." [Online]. Disponível: http://www.iso.org/iso/catalogue_detail.htm?csnumber=50942 [Acessido a: 2015-09-03]

[34] "ISO/IEC 15693-1:2010 - Identification cards – Contactless integrated circuit cards – Vicinity cards – Part 1: Physical characteristics." [Online]. Disponível: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39694 [Acessido a: 2015-09-03]

[35] "ISO/IEC 15693-2:2013 - Identification cards – Contactless integrated circuit cards – Vicinity cards – Part 2: Air interface and initialization." [Online]. Disponível: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39695 [Acessido a: 2015-09-03]

[36] "ISO/IEC 15693-3:2014 - Identification cards – Contactless integrated circuit cards – Vicinity cards – Part 3: Anticollision and transmission protocol." [Online]. Disponível: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43467 [Acessido a: 2015-09-03]

[37] "ISO / IEC TR 18001: 2004 - Tecnologia da Informação - de identificação por freqüência de rádio para o gerenciamento de itens - perfis de requisitos de aplicação." [Online]. Disponível: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40733 [Acessido a: 2015-09-03]

[38] "ISO/IEC 18000-1:2008 - Information technology – Radio frequency identification for item management – Part 1: Reference architecture and definition of parameters to be standardized." [Online]. Disponível: http://www.iso.org/iso/catalogue_detail?csnumber=46145 [Acessido a: 2015-09-03]

[39] "ISO/IEC 18000-2:2009 - Information technology – Radio frequency identification for item management – Part 2: Parameters for air interface communications below 135 kHz." [Online]. Disponível: http://www.iso.org/iso/catalogue_detail.htm?csnumber=46146 [Acessido a: 2015-09-03]

[40] "ISO/IEC 18000-3:2010 - Information technology – Radio frequency identification for item management – Part 3: Parameters for air interface communications at 13,56 MHz." [Online]. Disponível: http://www.iso.org/iso/catalogue_detail.htm?csnumber=53424 [Acessido a: 2015-09-03]

[41] "ISO/IEC 18000-4:2015 - Information technology – Radio frequency identification for item management – Part 4: Parameters for air interface communications at 2,45 GHz." [Online]. Disponível: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62539 [Acessido a: 2015-09-03]

[42] "ISO/IEC 18000-6:2013 - Information technology – Radio frequency identification for item management – Part 6: Parameters for air interface communications at 860 MHz to 960 MHz." [Online]. Disponível: http://www.iso.org/iso/catalogue_detail.htm?csnumber=46149 [Acessido a: 2015-09-03]

[43] "ISO/IEC 15961:2013 - Information technology – Radio frequency identification (RFID) for item management – Data protocol: application interface." [Online]. Disponível: http://www.iso.org/iso/catalogue_detail?csnumber=30528 [Acessido a: 2015-09-03]

[44] "ISO/IEC 15962:2013 - Information technology – Radio frequency identification (RFID) for item management – Data protocol: data encoding rules and logical memory functions." [Online]. Disponível: http://www.iso.org/iso/catalogue_detail.htm?csnumber=43459 [Acessido a: 2015-09-03]

[45] "O que é NFC?" [Online]. Disponível: http://www.techtudo.com.br/artigos/noticia/2012/01/o-que-e-nfc.html [Acessido a: 2015-02-26]

[46] "O que é NFC (Near Field Communication)?" [Online]. Disponível: http://www.infowester.com/nfc.php#funcionamento [Acessido a: 2015-02-26]

[47] "ISO14443A - NFC Tools." [Online]. Disponível: http://nfc-tools.org/index.php?title=ISO14443A [Acessido a: 2015-10-05]

[48] "Cartão Ultralight Gloss - NFC." [Online]. Disponível: https://www.nfc.pt/home/23-cartao-ultralight-gloss.html [Acessido a: 2015-06-17]

[49] "Arduino - Home." [Online]. Disponível: http://www.arduino.cc/ [Acessido a: 2015-02-26]

[50] "Raspberry Pi." [Online]. Disponível: http://www.raspberrypi.org/ [Acessido a: 2015-02-26]

[51] "BeagleBoard.org - black." [Online]. Disponível: http://beagleboard.org/BLACK [Acessido a: 2015-02-26]

[52] "Arduino uno." [Online]. Disponível: https://upload.wikimedia.org/wikipedia/commons/7/71/Arduino-uno-perspective-transparent.png [Acessido a: 2015-06-17]

[53] "Conhecendo o Raspberry Pi Modelo B - Especificações - Raspberry Pi Brasil." [Online]. Disponível: http://raspberrypibra.com/conhecendo-o-raspberry-pi-modelo-b-especificacoes-336.html [Acessido a: 2015-06-17]

[54] "BeagleBone Black Review | Linux User & Developer - the Linux and FOSS mag for a GNU generation." [Online]. Disponível: http://www.linuxuser.co.uk/reviews/beaglebone-black-review [Acessido a: 2015-06-17]

[55] "Arduino UNO." [Online]. Disponível: http://www.inmotion.pt/pt/arduino-boards/435-arduino-uno-rev-3.html [Acessido a: 2015-06-17]

[56] "Raspberry Pi 2 with 8GB Class 10 NOOBS Card." [Online]. Disponível: http://www.inmotion.pt/pt/boards-and-kits/1152-raspberry-pi-2-with-transcend-8gb-class-10-noobs-card.html [Acessido a: 2015-06-17]

[57] "BeagleBone Black." [Online]. Disponível: http://www.inmotion.pt/pt/beagleboard/800-beaglebone-black-rev-c.html?search_query=beagle&results=14 [Acessido a: 2015-06-17]

[58] Philips, "PN532/C1." [Online]. Disponível: http://www.adafruit.com/datasheets/pn532ds.pdf

[59] "miniLector Air NFC." [Online]. Disponível: http://www.bit4id.com/pt/index.php?option=com_content&view=article&id=123&Itemid=573 [Acessido a: 2015-06-17]

[60] "Adafruit PN532 NFC/RFID Controller Shield for Arduino with Extras." [Online]. Disponível: http://www.inmotion.pt/pt/adafruit/902-adafruit-pn532-nfc-rfid-controller-shield-for-arduino-with-extra.html?search_query=pn532&results=2 [Acessido a: 2015-06-17]

[61] "Bit4id-Comercio Electrónico." [Online]. Disponível: http://www.bit4id.com/online_store_es_pt/Bit4id_Tienda_pt/index.php?gen=20 [Acessido a: 2015-06-17]

[62] "Adafruit PN532 NFC RFID Controller Shield for Arduino + Extras." [Online]. Disponível: http://www.ptrobotics.com/rfid/3073-adafruit-pn532-nfc-rfid-controller-shield-for-arduino-extras.html [Acessido a: 2015-06-17]

[63] "Proximidad Mifare - Dactilplus Biometria." [Online]. Disponível: http://www.dactilplus.com/proximidad-mifare.html [Acessido a: 2015-03-02]

[64] "RFID Reader ID-12." [Online]. Disponível: http://www.inmotion.pt/pt/em4100-125khz/111-rfid-reader-id-12la.html [Acessido a: 2015-06-17]

[65] "RFID Reader ID-20." [Online]. Disponível: http://www.inmotion.pt/pt/em4100-125khz/938-rfid-reader-id-20la-125-khz.html [Acessido a: 2015-06-17]

[66] "RFID – ID-12 & ID-20." [Online]. Disponível: http://medialappi.net/lab/equipment/sensors/id-12-id-20/ [Acessido a: 2015-06-17]

[67] "Products - ID ISC.PR101-A." [Online]. Disponível: http://www.feig.de/en/products/obid/product-areas/obid-i-scan-hf/proximity-readers/id-iscpr101-a-proximity-reader.html [Acessido a: 2015-06-18]

[68] FEIG ELECTRONIC, *HF Proximity Reader ID ISC.PR101*, 2012.

[69] "RFID - ID ISC.PR101 13,56MHz Proximity Reader." [Online]. Disponível: http://www.rfid-webshop.com/product_info.php/info/p302_ID-ISC-PR101--13-56MHz-Proximity-Reader.html/XTCsid/15dd [Acessido a: 2015-06-18]

[70] "bind." [Online]. Disponível: http://pubs.opengroup.org/onlinepubs/009695399/functions/bind.html [Acessido a: 2015-06-21]

[71] "TCP/IP Network Programming Design." [Online]. Disponível: http://vichargrave.com/network-programming-design-patterns-in-c/ [Acessido a: 2015-06-21]

[72] "I2C Installation for Raspberry Pi – Step by Step Guide | SK Pang Electronics Ltd." [Online]. Disponível: http://skpang.co.uk/blog/archives/575 [Acessido a: 2015-04-30]

[73] "Libnfc - NFC Tools." [Online]. Disponível: http://nfc-tools.org/index.php?title=Libnfc [Acessido a: 2015-04-30]

[74] "Libnfc:quick start example - NFC Tools." [Online]. Disponível: http://nfc-tools.org/index.php?title=Libnfc:quick_start_example [Acessido a: 2015-04-30]

[75] "NFC on RaspberryPi with PN532, py532lib and i2c." [Online]. Disponível: https://blog.adafruit.com/2012/11/23/nfc-on-raspberrypi-with-pn532-py532lib-and-i2c-piday-raspberrypi-raspberry_pi/ [Acessido a: 2015-02-26]

[76] "Max3232." [Online]. Disponível: http://www.doc-diy.net/electronics/rs232plug/ [Acessido a: 2015-06-23]

[77] "RPi Serial Connection - eLinux.org." [Online]. Disponível: http://elinux.org/RPi_Serial_Connection#Connection_to_a_microcontroller_or_other_peripheral [Acessido a: 2015-06-23]

[78] "Raspberry Pi and the Serial Port." [Online]. Disponível: http://www.hobbytronics.co.uk/raspberry-pi-serial-port [Acessido a: 2015-06-23]

[79] "Serial Programming." [Online]. Disponível: http://tldp.org/HOWTO/Serial-Programming-HOWTO/x115.html [Acessido a: 2015-04-16]

[80] a. T. I. Technology, *Tag-it HF Transponder Inlays Reference Guide*, 2001, no. December 2005.

[81] "Botão de pressão." [Online]. Disponível: http://www.eletronicalowcost.com/index.php?route=product/product&product_id=120 [Acessido a: 2015-06-23]

[82] "pigpio library." [Online]. Disponível: http://abyz.co.uk/rpi/pigpio/download.html [Acessido a: 2015-04-29]

[83] "How To Install Linux, Apache, MySQL, PHP stack on Debian | DigitalOcean." [Online]. Disponível: https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-on-debian [Acessido a: 2015-05-18]

[84] "MySQL :: MySQL 5.0 Reference Manual :: 6.3.4 Setting Account Resource Limits." [Online]. Disponível: https://dev.mysql.com/doc/refman/5.0/en/user-resources.html [Acessido a: 2015-06-24]

[85] "Páginas Web." [Online]. Disponível: http://www.clomputech.com/paginas-estaticas-vs-dinamicas.html [Acessido a: 2015-06-24]

[86] "PHP ou Javascript? Qual a diferença?" [Online]. Disponível: https://ahaprogramando.wordpress.com/2008/04/05/php-ou-javascript-qual-a-diferenca/ [Acessido a: 2015-06-24]

[87] "Permissão na pasta www em ubuntu." [Online]. Disponível: http://www.vivaolinux.com.br/topico/Particoes-no-Linux/Permissao-na-pasta-www-em-ubuntu [Acessido a: 2015-04-29]